

高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議
技術戦略専門委員会
第4回会合議事要旨

1. 日時 平成17年11月4日(金) 10:00~12:00

2. 場所 内閣府本府第5特別会議室

3. 出席者

[委員長]

佐々木 良一 委員長(東京電機大学教授)

[委員]

志方 俊之 委員(帝京大学教授)

篠田 陽一 委員(北陸先端科学技術大学院大学教授)

田尾 陽一 委員(セコム株式会社顧問)

中西 晶 委員(明治大学助教授)

西尾 章治郎 委員(大阪大学大学院教授・文部科学省科学官)

米澤 明憲 委員(東京大学大学院教授)

(五十音順)

[政府]

内閣官房情報セキュリティセンター副センター長

内閣官房情報セキュリティセンター情報セキュリティ補佐官

内閣官房情報セキュリティセンター内閣参事官

警察庁情報通信局情報技術解析課長

防衛庁長官官房情報通信課情報保証室長

総務省情報通信政策局情報通信政策課情報セキュリティ対策室長(代理:同室課長補佐)

文部科学省大臣官房政策課情報化推進室長

経済産業省商務情報政策局情報経済課情報セキュリティ政策室長

4. 議事概要

(1) 技術戦略専門委員会報告書(案)について

事務局より説明

(2) 技術戦略専門委員会報告書(案)についての討議

【副題、はじめに】

副題は中身を示唆する。技術戦略専門委員会という組織の名前から、抽象的だが、「戦略的な研究開発・技術開発の推進」などが良いのではないか。

「戦略的推進」が良い。また、略語があった方が良い。

研究開発・技術開発の推進の総合的デザインとか、国家的デザインとか、デザインという言葉も副題に入れるべきではないか。

副題は「推進戦略」とか「デザイン」が良い。「新たな推進」では弱い気がする。「はじめに」は3ページもあって読むのがつらい。小見出しを付けるべき。

【1．情報セキュリティ技術戦略を考える上での基本的な考え方】

ここのポイントは、全体を表す図が入ったこと。これにより報告書の全体が分かりやすくなった。

「組織・人間系の管理手法」については、前回まで出てきた「社会科学」という言葉よりはかなりターゲットは絞れてきたのではないか。

その書き方については、他の項目と次元を合わせるという趣旨で、もっと展開した方が良いのではないかと思う。

展開して書き下すためには、組織・人間系の管理手法の高度化に取り組む際の研究の留意点について、知見が必要となる。これについては、知恵を出していただきたい。

社会システムデザインが環境整備の中に入っているが、社会システムデザインはもう少し上部の概念ではないのか。社会システムデザインがはっきりしないから情報セキュリティ対策が進まない、という気がする。周りを取り巻く環境整備ではなく、技術系の人でも人間系の人でも突っ込んで、新しいサービス構造に転換するデザインングに注力するべきではないか。そのときに、セキュリティをこうやって守る、法律をこうする、といったことを議論し、それを受けて技術をどうするか、人間系をどうするか、ということを考えるべきという気がする。

深さの問題はどこかで言わなくてはいけない。総合科学技術会議やIT戦略本部などで本来決まっているべきものが、実は決まっていないので我々が苦労している。そういうところに向かって、「早くやれ」と伝えることが大事。とはいえ、別な章を立てて「社会システムデザイン」を書き始めると大変なことになるので、そこまでやる必要はない。書き方の問題だと思う。

そうしたことは「はじめに」で書くべきかも知れない。

会社でCIO、CISOをやっていると、経営者が次のサービスを考えているときに、システムをどうするか、セキュリティをどうするか、ということに責任を負わなければならない。今あるシステムの脆弱性をどうしよう、ということもあるが、新しいサービスを始めるときにそこに内在する脆弱性のケア、というのが難しい。穴が開いてから気が付く、ということも割とあると思う。

「はじめに」にはパーセプションしか書けないので、問題意識のふんわりしたことを書き込み、1.4(1)「社会システムデザイン研究の実施」をもう少し厚くするとともに、3.2(1)「社会システムデザインに関する研究促進」で内閣官房が他のところに働きかけるような書きぶりとすることで良いか。

「はじめに」については、今の中身を足すかどうかは別にして、上手く書けていると思う。ただし、「参考」については、これを読んで認識を新たに出来るところがあるので、情報セキュリティの特殊性、特異性について、1章の1.1の前に組み込んだ方が良い。

あくまで参考としてまとめたのは、他の委員会に係るものだからということ。総合科学技術会議の検討における安全・安心領域の書き方と、技術との関係を浮き彫りにするために書いているという位置付け。

情報セキュリティの特殊性として、発生シナリオ自身が変わってくるということはあるので、それは1章の頭に混ぜ込む。

1章の中で、「1.1」と「1.2」「1.3」との関係が分かりにくい。

1.1と1.2は無くてもいいセクションと思っている。しかし、これが無いと、これまで何もやってこなかったのか、研究領域は何なのかが見えないのではないかと、ということで、イントロとしてここに持ってきている。

基本構造としてそれで良い。1.3以降がこのレポートの大事なところと理解した。1.3(1)で「利用者が安全であると分かること」を目標としているが、それを明確にサポートするものが何か、というのが分からない。

3.1の「IT要因によるリスク評価の研究」や「情報セキュリティ評価技術の研究」がその出口となると考えている。

報告書の全体図は分かりやすくいいが、右側で矢印が上に上がっていくのが違和感がある。また、「ここだけ読めば全体がわかる」というのが重要。その観点から、この図は横になってしまっても良いので、A4一枚くらいにして、もっと前に持っていったほうが良い。

脅威が書いてあるが、これが1ページしかなく、しかもいきなりDDOSやBOTなどの細かい話になっている。国家がどれほど危険にさらされているか、という観点で、社会的脅威、国家的脅威ということを強調した方が良い。

サマリー版を作ることを予定している。また、本文の記述に関しては、上手く前の方に入れていくように書き換える。

【 2 . 情報セキュリティ技術の研究開発・技術開発の新しい推進構造のあり方】

「推進構造」は一般的な言葉なのか。「構造の構築」も気になる。

独立行政法人の主な役割についてはこの表現で良いのか。独立行政法人は本来、独立性をもってミッションをこなしていくという組織なので、このように書いてしまうと独立行政法人としても何かギクシャクするものがあるのではないか。

ここは独立行政法人がやられている研究のことを書いているのではなくて、産官学の共同プロジェクトを実施するときにそれぞれの役割があるわけで、それを果たして下さいと書いているということ。

とげとげしい部分がある。「現在のレベルよりも下げ」は修正すべき。「現在のレベルに保ちつつ」ぐらいでどうか。

ご指摘の、このレベルの部分については削除することとしたい。

各章の分量のバランスが悪い。1章が長すぎる。

事務局内の議論において、「技術とは何か」「総合科学技術会議との関係は」というのが議論になった。その説明のためにどうしても1章が厚くならざるを得ない。その後の章はシャープかつクリアにやるべきことを書いているため、厚さが変わってくる。

【 3 . 情報セキュリティ技術開発の重点化と環境整備のあり方】

デジタルフォレンジックが萌芽的研究なのか、という気もするが、大事なのは、情報の証拠性をどのように確保し、その証拠性を提示していくかということ。そのあたりを書いておく必要がある。

電子認証技術についてもかなり具体的に書かれているが、そういったレベルならば、タイムスタンプなど、ロングタームなセキュリティの確保も入れておくべき。

「GRID」については、「GRID」という語を使わずに書く努力をしてみたが、説明的になりすぎてしまい、固有名詞を出さざるを得なくなっている。

報告書が出ると、みんな分かりやすいところに飛びつく。この報告書案では、「フォレンジック」や「DDOS」「GRID」に視線が集中するのではないか。

「GRID」は単に数理科学のみならず、社会科学を含む言葉なので、このくらいは書いても良いのではないかという気がする。

「高信頼性組織構築」については、「高信頼性組織デザイン」と書くと良いのではないか。

「IT要因によるリスク評価の研究」、「情報セキュリティ評価技術の研究」は評価で終わるのではなくて、目標である「ITが安全であると分かること」との関係から、何らかの形が欲しい。

「萌芽的研究」としては、萌芽的といえるかわからないが、トラステッドコンピューティングやセキュアOSがありうるのではないかと。あと、蒸し返すが「GRID」という語は出すぎ。

カタカナ語や略語はフルスペルを書くべき。英語の原語は日本語訳を付けるべき。

GRIDの日本語訳は無かったのではないかと。「先進的な分散環境」とでもするか。

「基礎研究領域」としては、ロジック、検証技術やリーズニングなどが入るのではないかと。

「基礎研究領域」には「暗号」という言葉は書いていないが、それで良いかと。応用数学と情報理論、符号理論の答えとして暗号が出てくると考えている。

暗号で使われる離散数学は応用数学ではないと考えている。

「人材育成」のところでは、人材育成を行うための土壌として、セキュリティは暗くないということを入れていただきたい。

明るい、暗い、は別にして若者の理系離れに触れるべきかと考えている。あと、最近ではIT離れという傾向もある。

セキュリティが暗いのはディフェンシブであるから。「守る」一方だとどうも元気が出ない。

理系離れを防ぐという意味では、我々の日常生活の安全性を守るという重要性を謳うことによって、セキュリティの重要性を認識してもらうことが必要ではないかと。

セキュリティが持つ積極的な面として、セキュリティ技術があるから実現した、ということについても何か触れたい。

自分が国を守る、セキュリティを守るという使命感、倫理観を認識させる表現が必要。人材育成のところでは「技術を持ちつつ、使命感を持った人材を育成する」ということを明示することが大事。

【4.「グランドチャレンジ型」研究開発・技術開発の推進】

「情報セキュリティユニバーサルデザイン」については、その定義はその前に書いてある説明ということで良いか。

そのとおり。ただし、情報セキュリティユニバーサルデザインという言葉は、まだ一般語にはなっていないのでカッコを付けた方が本当は良いと思う。

グランドチャレンジということで色々考えていたが、例えば、ウイルスの脅威の根絶というのは20年たっても難しいのではないかと思っている。明示的に明確なゴールを置くのが難しい気がしている。

ご指摘は全くそのとおり。このため、「継続的にグランドチャレンジにふさわしいテーマを検討するため」という言葉を置いている。情報セキュリティにおいては、それを検討することが大きなバリュー。その中でテーマが見出されれば、それに着手することで、大きな副次的効果も得られると思う。しかし、「Man to the Moon」のような単純なテーマを情報セキュリティにおいて設定することは困難。したがって着手すら難しいと思うが、そのテーマを継続的に検討していくことによる成果を得ていきたい。

グランドチャレンジは、どの程度の規模を考えているのか。インターナショナルにリードするようなテーマは、国に閉じる話ではないと思っている。

似たような言葉で「探索的研究」というのがある。そんなこと出来ないだろうというのをシコシコやっていると、新しい世界が見えてくる。一方、グランドチャレンジはカネとヒトとモノをチャレンジブルにどーん入れれば出来る元気印のようなもの。

大目標を立てて判りやすくすることが大事。テーマとして例示されている3つのうち、2つ目、3つ目は分かりにくい。2つの目の「エラーの最小化」は弱い。「エラーを根絶する」とすべき。3つ目は何となく出来てしまいそうな気がする。

「探索的研究」は、基礎研究領域のところに入れたら良いのではないか。

「Man to the Moon」がうまいな、というのは、税金を投入するに当たり、国民が夢を得られて理解される、ということ。そういう観点からの意味合いも必要だと思う。

先ほどのご指摘の3つ目のテーマについては、本当は「迷惑電話のない世界」と書きたかった。分かりにくいので、表現については再考する。

【全体として】

「情報のセキュリティ」には2種類あり、アイデンティティの評価をすることで安全

・安心をつくる、というのと、アノニミティを作ることで社会の自浄作用をサポートし、社会の安全安心を作る、ということだと考えている。

こうした点について、本報告書で触れるかどうか伺いたい。

この報告書案全体として、プライバシーの記述が少ない。

匿名性の分かりやすい例としては電子投票がある。最終的に誰が何を投票したか分からないようにする。

1.4の環境整備に新しい項を立てて、プライバシーあるいは人間系との連関の中での情報セキュリティ技術の役割について書く。その中身はプライバシー、アイデンティティ、アノニミティとする。その具体は3.2(5)にプライバシーコンシャスな情報処理や電子投票の実現などを書く、としてはどうか。

安心と安全の関係として、安全であること、安全であることが分かること、万が一事故が起こった場合でも被害の局限化や救済等が図られること、となっているが、これについてはこの委員会の中でコンセンサスが取れていると理解して良いのか。そうであるならば、今後の参考としたい。

3つ目の、万が一事故が起こった場合でも被害の局限化や救済等が図られることについては、万が一の際にも経済活動が維持できる、事業が継続できるというニュアンスが入ると良いと思う。

安心と安全の3つの項目については、エクスプリットには議論はしていないが、このような形ではないかということで進めて来ているものと理解している。

日本では、「個人情報」ということで災害時要支援者の情報が取りにくくなっているが、韓国では要支援者にはICタグに支援に必要な情報を入力し、持ち歩かせているので救命率が高いとのこと。今ある技術で出来ることもあるので、遠い戦略とともに今現在の戦略もやって欲しいと思う。

(3) 今後の予定

事務局より説明

以上