

基本計画検討委員会(2月14日)ヒアリング提出資料

国立情報学研究所

教授 浅野正一郎

(重要インフラ専門委員会委員長)

◆第1次基本計画の下での重要インフラの取組みについて

・「重要インフラの情報セキュリティ対策に係る行動計画」(2005年12月13日・情報セキュリティ政策会議決定)に基づき、別紙のとおり取組みを推進しており、全体としては、重要インフラの情報セキュリティ対策は着実に向上しているものと認識している。

・今年度末までに各重要インフラ分野にCEPTOARが整備されるなど、重要インフラ横断的な情報共有体制の整備は進んでいるが、現実には情報がスムーズに流通するまでには、まだ時間を要するよう思う。

・重要インフラの情報セキュリティ対策はPDCAサイクルの下で向上していくことになり、妥当なサイクルの運用や事業者レベルのPDCA意識の啓発へと議論は進みつつある。

・次期基本計画の検討と時期を合わせて、「行動計画」の見直しも開始されている。現在の計画は走りながら作ったものであり、実情と合わないところもあってしかるべきだと認識している。実際の事業者の意見等も聞きながら、実情の沿った修正をするのが適切と考える。

◆情報セキュリティ対策の推進に当たり留意すべき事項


重要インフラにおける情報セキュリティ対策を実効的に推進するためには、特に以下の実情についての認識も必要。(重要インフラ専門委員会における議論を参考に私見を交えている)

- ・ITへの依存度合いは、重要インフラ分野、重要インフラ事業者ごとに多様である。
- ・重要インフラ事業者としての現実の意思決定には、経営、内部統制、コンプライアンスなど、情報セキュリティ以外の視点も重要な要素である。
- ・重要インフラ事業者にとっては、他の重要インフラ事業者との連携よりも、自らの「顧客」対応を優先せざるを得ない場合が現実に存在する。
- ・大規模IT障害の波及防止とともに、機能回復に必要な措置についても視点を広げることが望ましい。

◆今後の情報セキュリティ対策の方向性について

- ・重要インフラ事業者にとって、利用者のための「事業継続」「サービスの維持」が最大の課題。そのために必要な対策に重点をおくべき。
- ・重要インフラにおける情報セキュリティ対策の基本は、あくまでも各事業者の自律・自主的な取り組み。「やらされる」対策では実効性は上がらない。
- ・重要インフラ防護という目的に照らすと、政府の対応としては「防災」の取り組みとの連携が不可欠。
- ・社会全体的な情報セキュリティの向上のために、「内閣官房情報セキュリティセンター」という機能をもっと有効に活用することを考えるべき。また利用者(国民・企業)との接点を示し、利用者の視点に沿ったBCP作成を支援するなどの将来的事項への対応も忘れることができない。

現行動計画の下での取り組みの概要



重要インフラの情報セキュリティ対策に係る行動計画
(2005年12月13日情報セキュリティ政策会議決定)

【4つの柱】

- 1. 「安全基準等」の整備
- 2. 情報共有体制の構築
- 3. 相互依存性解析の実施
- 4. 分野横断的演習の実施

