資料５－３

【三輪委員御意見】

昨日の委員会では討議の時間が十分ではなかったために、本メールにて
私の意見を述べさせて頂きます。

１．卓上資料２のＰ．１について

文中にある１０分野とは別に協力を求める業界について、ＩＴ業界、情報セキュリティ業界が横断的に関わる必要性があると思われます。

また、電力、物流の分野においては石油化学コンビナートに代表される燃料生成・備蓄などの大規模プラント業界も深く関連すると思われます。

参考：平成１１年「石油プラントのネットワーク安全性検証実験」

２．卓上資料２のＰ．７について

＜当日の発言のまとめと補足＞

Ａの「c.予兆・警報に関する情報」において、国内外の犯罪組織やテロ組織の情報や現在一般企業に行われているネット犯罪の情報、技術的な対策情報、サイバー空間に閉じたもの、サイバー空間から物理的人的攻撃を可能とするサイバーテロの研究成果などの情報を事案対処省庁は有していると考えられることから、これらの情報を取扱いを十分に検討した上で情報提供を受けるべきである。

Ｂフェーズにおいては、特にサイバー攻撃の場合には事案対処省庁が同時に初動を行うのは当然のことと考えます。情報共有のスキームとして欠落しているのは、これを見た事案対処省庁により日常的に治安を感じている一般国民には極めて不自然に感じると思われます。

また、法執行機関が入ることにより重要インフラへのセキュリティ事案対処が萎縮したり混乱する、という事務局からの意見については、警察庁からも「そのような暴挙」は行わない旨明言されました。

重要インフラにおける捜査活動などは★明らかに事業継続を優先★すべきであるものの、被害の拡大防止のためにはむしろ事案対処省庁による速やかな情報提供が行われてしかるべきと考えます。他国の失敗から学習し我が国ならではのモデルの構築に挑戦すべきではないでしょうか。

参考資料１－１のＰ．５における事案対処省庁の関わりについて、一歩踏み込んだ記述を期待します。

３．参考資料１－１及び１－２について

参考資料１－２の個別論点Ｐ．３９において、事案対処の観点からの課題検証が述べられており、上記の情報共有の枠組みに事案対処省庁の参加が当然であろう、という考えに基づくと、参考資料１－１のＰ．４において、分野横断的な演習の実施における主体に事案対処省庁が加わり積極的な情報提供に務めることは欠かせない要素と考えます。

その意味からすると、「相互依存性解析」とは別に本来の「サイバー攻撃を想定した分野横断的演習」を設定する必要があります。その中には、机上演習だけでなく、高度な技術を駆使した演習も行われなければならず、そのためには日頃からのサイバーテロ技術の専門研究機関が必要であることが必要であります。これは事案対処省庁では既に行われているものの、業界の制御ネットワーク情報などの協力があればより効果的となります。

以上長文失礼しました。