資料１

サイバー対処能力強化法の施行等に関する有識者会議（第２回）ヒアリング資料

日本労働組合総連合会
総合政策推進局長　冨田　珠代

重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針（骨子たたき台）に対する意見

【総論】

・サイバー対処能力強化法に基づく「官民連携」は、「重要電子計算機に対する不正な行為による被害の防止をはかる」という法の目的達成のために行うものであるため、国が主体的な役割を担うとともに、内閣府・関係行政機関と事業者等との役割分担を明確にお示しいただきたい。

・本法の義務が課される民間事業者は「特定社会基盤事業者」となっているが、「特定社会基盤事業者」がシステム開発を行う場合、２次請け企業と共同で行う事があるが、インシデント発生時の２次請け企業の対応がどうなるのか、お示しいただきたい。

・わが国のサイバーセキュリティを強化するには、官民の情報共有だけでなく、サイバーセキュリティに関わる人財の育成やスキル向上が必要であり、国による研修など支援体制も検討いただきたい。

【各論】

〇第１章　第３節　事業者等との連携

・事業者等は、サイバー対処能力強化法にもとづく新たな対応を社内規定やマニュアルなどに反映する必要が生じるが、その際、行政機関によって対応が異なることのないよう、政府として標準的な事項をお示しいただき、実務者の負担軽減に努めていただきたい。

〇第１章　第４節　通信の秘密の尊重

・通信情報の取得にあたっては、国民の権利と自由が不当に制限されることのないよう、法第１条に規定の通り、取得対象は真に必要な通信情報に限りなく限定するとともに、取得情報の対象を広げる際のルールについても明確にしていただきたい。

・また、通信の秘密を制限することの妥当性や対象情報の範囲を国民に丁寧に説明するとともに、取得した通信情報の流出・目的外流用の防止策と万が一流出した場合の国民への情報公表のあり方などについても明確にしていただきたい。

〇第４章　第１節（１）特定重要電子計算機の届出の考え方

・特定重要電子計算機の届出対象は、真に必要かつ特定社会基盤事業者が現実的に管理対応可能な範囲となるよう、特定社会基盤事業者との意見交換を丁寧に実施いただきたい。特に、更新頻度の高いＯＳのバージョンや適応パッチ、アプリケーションとそのバージョンなどを対象とすることは、管理者の負担軽減の観点からも慎重に検討いただきたい。

〇第４章　第１節（２）特定侵害事象等の報告の考え方

・インシデントは、既に個別業法に基づき所管省庁へ報告が義務付けられているものもあるため、本法に基づく報告と個別業法に基づく報告の役割分担を明確にお示しいただきたい。
・また、発生したインシデントによって報告先が異なると現場の負担が増えるため、報告窓口を所管省庁に一本化し、政府内で連携いただく体制をつくることなども検討いただきたい。
・インシデント発生時はインシデント対応に注力する必要があるため、インシデント報告のタイミングについては、たたき台に記載の通り、事業者や労働者の過度な負担とならないことを十分の考慮の上で設定いただきたい。

〇第４章　第３節　関係機関等への協力の要請

・サイバー攻撃の被害や全容把握のための情報収集は必要であるが、収集・集約する情報の精度などをあげるために、事業者等に対して追加の情報提供を求めるなど、過度な負担を強いることの無いよう留意いただきたい。あわせて、収集・集約した情報の管理を徹底いただきたい。

〇第６章　第５節　守秘義務・安全管理措置の具体的内容

・協議会の構成員は、特定社会基盤事業者だけでなく、自治体や個人なども対象となりうるとの事なので、安全管理措置の具体的内容を検討する際は、安全管理措置を科す範囲についても明示していただきたい。
・情報漏洩を防ぐには、構成員が協議会で共有される情報の取り扱いに迷いを生じさせないことが何よりも重要である。そのため、協議会が求める「守秘義務」の内容を構成員に明示するとともに、構成員へ守秘義務教育の徹底を求めることなども検討すべきと考える。
・また、協議会では秘匿性の高い情報を構成員が取り扱えるよう「セキュリティ・クリアランス制度の活用も検討する」とされているが、セキュリティ・クリアランス

制度は、本来、守られるべき個人のプライバシー情報を調査するため、検討の際は、協議会の構成員にセキュリティ・クリアランスの取得を強要しない制度としていただきたい。

以上