第４回会議の議論の整理（主なポイント）

資料１

１．セキュリティ・クリアランス制度へのニーズ、あるべき方向性

（１）国際的なビジネス・共同開発等でのニーズ

- あるサイバーインシデント事案の現場に直接赴いたことのある海外の方と面談する機会があり、そのときの情報と我々が得ていた情報とのギャップの大きさ、詳細さに非常に大きな差があった。いかに詳細な一次情報にアクセスできるかが、重要インフラ事業者の設備・システムを守るために非常に重要。そのためには、セキュリティに関する海外の国家機関や事業者との情報交換を行うに当たり、セキュリティ・クリアランスが必要になると考えている。
- サイバーセキュリティ情報について、官民で協力する際、機密情報を解除することもアメリカでは行っているようであり、民間との秘密情報の共有が進んでいくと思われる。他方で、これらの情報はアメリカ国内でも厳格に管理されているであろうから、仮に、こうした情報がアメリカの現地法人で入手できるようになったとしても、これらを日本本社に共有することが難しいのではないかと思う。
- アクティブ・サイバー・ディフェンスについては、事業者に協力義務をかけようとすると法的な手続きが必要となるし、これに伴う従業員に対する人的なセキュリティ・クリアランスも必要となってくる。
- 国際連携に影響が生じる可能性のある分野として宇宙がある。例えば、相手国のシステム等と連携しようとする際、相手国のシステム等の仕様の提案要件の中にＣＵＩ（Controlled Unclassified Information）のみならずＣＩ（Classified Information）が含まれる場合があり、セキュリティ・クリアランスを取得しないと、連携が出来ないということが考えられる。

（２）情報保全の必要性

- 災害や事故があって使えなくなると国民生活に直結するような重要インフラ事業者は、世界中で今どんな攻撃、マルウェアがあるのかというのはただちに知りたいはずで、防御策についても国と共有したいだろう。そうなると会社できちんとした体制を整えて、それがセキュリティ・クリアランスになるのだろうが、国としてそういう方向に向かうべきなのではないかと考える。
- サイバーセキュリティに関して、産業界のニーズに加えて国としてのニーズもあることがはっきりしたのではないか。
- 重要インフラ事業者のうち、競合関係にある企業とは信頼は成立しないが、個社間で信頼関係が成立する会社とは情報交換をしている。ただ、情報量とその多様性に限界があり、政府が保証する情報共有に期待するところはある。一方で、官民の情報共有の活性化には、秘密保持のルールをしっかり作っていただき、情報共有に伴うリスクへの懸念をぜひ払拭してもらいたい。

第４回会議の議論の整理（主なポイント）

１．セキュリティ・クリアランス制度へのニーズ、あるべき方向性

（３）国際的な枠組み

- 政府間の枠組みの下で、ヨーロッパやアメリカの国家機関と日本の民間企業との情報交換が可能となるような関係性を構築していただきたい。特にファイブ・アイズのヨーロッパやアメリカの政府機関との連携は切にお願いしたい。
- サイバーセキュリティ情報について、仮に日本のセキュリティ・クリアランス制度が整備され、諸外国と相互認証されても、民間企業が政府を経由せず海外政府に直接データを提供してもいいのかという問題がある。日本政府を通じてアメリカ政府に情報を提供する必要があるとなると、これは単にセキュリティ・クリアランスの問題に留まらず、日本とアメリカの政府間でルートを開かないと、双方でレシプロカルにはできない。

第４回会議の議論の整理（主なポイント）

２．ニーズにこたえるための制度設計の方向性

（１）調査とプライバシー・従業員との関係

- セキュリティ・クリアランスは背景調査を伴うものなので、人権問題と常に裏腹である。背景調査を求める場合には、これを民間の裁量に任せるのではなく、政府の責任において、明確な制度を法制度上担保してほしい。背景調査を求める場合は、政府の責任で調査してほしい。
- 国の必要性に基づいて実施するセキュリティ・クリアランス制度であれば国の方できちんと調査をするべきであろう。他方、ビジネスのために企業がやりたければ、企業が自らの責任において同意を得た上で調査を実施することになるであろう。
- 我が国の法制では、官民どちらが調査を行うにしても本人の同意は絶対に必要であり、同意がなければできないと思う。
- ヒトゲノム・遺伝子解析研究等においては、対象者の単なる書面による同意だけでは不十分で、研究者が被験者に詳細な研究内容の説明を行うことや遺伝カウンセリングの機会を提供することなどが、国の指針で求められている。本テーマでも、「真摯な同意」をとるための方法について検討すべきかと思う。
- セキュリティ・クリアランスの際には、アメリカでもそうだと思うが、基本的に身上調査票を埋めていただくという作業があると認識している。従って、特定秘密保護法においてはそうした作業についての説明をしなければならないことになっていて、運用基準では同意にあたっての説明事項が規定されていると理解している。同意書の様式もあるかと思う。常識的な形で同意についてはさらっとやるというよりは、法律的に同意は明示されており、下位法令で更に様式的な形で担保しているという理解で良いかと思う。
- アクティブサイバーディフェンスに伴うセキュリティ・クリアランスであれば、これに協力する企業に対して、企業がやりたければ調査をやってもらうといった制度は無理があると思う。
- 機微な情報に直接アクセスをして、社として何をすべきなのかを判断し、部門内に指示できるだけの人数がセキュリティ・クリアランスを取得すればよいと考えており、それほど多くの人数は考えていない。
- ガイドラインに従い本人の同意のもと民間企業の人事部が調査した場合、アメリカが認めるかというとおそらく絶対に認めないだろう。政府や経済界の方々がアメリカ保有の情報、特にＣＩの共有を受けたい場合は、国の制度による背景調査が必要である。
- 民間企業が、今後、政府の定めるガイドラインと被用者本人の同意に基づいて実施できる可能性のある調査は、ＣＵＩのレベルにおけるバックグラウンドチェックに限られると思われる。

第４回会議の議論の整理（主なポイント）

２．ニーズにこたえるための制度設計の方向性

（２）情報の指定

- 根源的な問としてサイバーセキュリティにおけるインシデント情報は国家機密なのかという問題がある。サイバー攻撃は政府も攻撃されるし民間も攻撃される。インシデント情報やこれを惹起するマルウェア情報について、国が攻撃された場合は国が持っていて、民間企業が攻撃された場合は国家機密では無いということになってくる。また、インシデント情報は、発生してすぐ共有するのが重要。
- サイバーセキュリティについては、様々なプロトコルや防御についての情報があるところ、インシデント情報やマルウェアの特性がセキュリティ・クリアランスを付与しないとアクセスできない情報なのかどうかは整理する必要がある。
- 重要インフラに関するサイバー情報を共有するのにセキュリティ・クリアランスが必要となる場合がある。それは防御策である。インシデント情報の共有にセキュリティ・クリアランスを要するかについては確かに議論が必要だが、防御策は明らかになることで対策がなされてしまうと問題なので、機密（Top Secret）レベルのセキュリティ・クリアランスが必要かと思う。
- 仮に政府で被害を受けたものが第２回会議の事務局資料２「情報の区分（イメージ）」の「」「Ａ」に分類されたとしても、基本的に官であろうと民であろうとインシデント情報とそれに付随するものは開示することで防御に資する性質のものだと理解するのが正しいと思う。それに対する防御策も秘密の度合が高いので、それがどの領域にカテゴリーされるかは今後検討していくことだと思う。

（３）その他

- アメリカにおける企業等に関するＦＯＣＩ（Foreign Ownership, Control or Influence；外国による所有権・管理・影響）については、まだ我が国で十分な理解がされていないと思われる。これをチェックしないと、外国関係者による機密情報へのアクセスを排除することができない恐れが生じる。
- 第3回事務局資料２（諸外国制度比較）のどこの国も一定程度、むしろ日本と比べると相当数セキュリティ・クリアランス保有者が居るということが分かった。やはり安全保障の分野においてこういう制度・ニーズがあるということが分かった。