第２回目：セキュリティー人材政策の全体像について
実施日:２０１８年６月２２日（金）
発表者: 三角育夫氏（NISC 副センター長兼内閣審議官）

次期セキュリティ戦略の打出しと NISC における人材育成の取組
- サイバー空間の存在に対する社会的認識の変化
- IoT と AI の浸透化に伴うセキュリティーに対する社会的意識の変化
- 物理的時実空間とサイバー空間の一体化に伴い、社会に及ぼす脅威が深刻化
- 中・長期的な戦略（3 年間）７月中に閣議決定

サイバー空間のエコロジー的活用による社会経済的な発展
1.innovation への投資
- セキュリティのビジネスとしての価値創出
- サプライチェーンの実現による新しいビジネスへの可能性
- 安全性・信頼性の高い IoT 構築

2.国家治安・国民への安全性の提供
- 官民への安全を保証するための取組み
- 教育機関等における健全な教育・研究環境
- 政府機関・都道府県庁におけるセキュリティー強化

3.国際社会レベルにおける平和維持・国家の安全保障
- 自由かつ公平的ルールによるサイバー空間の管理・堅持
- 日本のサイバー脅威に対する状況把握力、防御力、抑止力の強化・向上
- 海外諸国との国境を超えた国際連携

上記施策打出しの主な背景
- IoT 機器のマーケット進出によるサイバー攻撃発生リスク（ボットなど増殖的攻撃による脅威）の急上昇
- 省庁・分野を超えた連携の必要性（サイバー脅威に関する攻撃・被害リスク、対応などについての情報共有、ネットワーク構築など）の必要性
- ２０２０年東京五輪に向けたセキュリティー・インフラ体制の整備の必要性

上記を実現させるため、人材育成・確保、研究開発、そして部門・管轄を問わず全員参加による協働を横断的施策として打出した。NISC による関係機関への働きかけ、各府省間の調整、産官学連携による政策モデルなど主導的役割を担う。

次期戦略実現に向けて、セキュリティー基本法を一部改定する方向でいることを明らかに

した。これは、日本の公共政策における情報収集・共有化の仕組みの不備や事故当事者に対する情報公表を巡る社会的制約が強く残っていることが主な背景となっている。そこで、NISC を事務局に専門家及び有識者による意見（パブリックコメント）などを対策情報源として国家行政機関、地方公共団体、重要インフラ業者、セキュリティー・システム関連事業者、教育研究機関などに迅速に共有し、各機関ごとに政策を連携・協働できるようなシステムを提案した。

セキュリティー対策は行政サービスを円滑に遂行するための justification であることを行政レベルで意識的に浸透させるべく、政府機関内における従来の情報セキュリティ対策における統一基準の見直しを打ち出した。

- 挙動検知による不正プログラムに拘る被害の未然（または被害拡大）防止

資産管理の自動化による脆弱性対応、情報漏洩対策の導入を政府機関主体で推奨する

- 国民が安心してウェブサイト等を用いて行政サービスを利用できるように利用者側に立った追加的対策を講じる。
- 政府機関レベルにおける自律的 PDCA サイクルの確立
- 独立行政法人などで独自に提供しているサイバーセキュリティー対策を導入

サイバーセキュリティ人材育成における取組み方針

ビジネスサービス、物作り、資産価値創出の観点からセキュリティ対策を事業として取込むべく、会社・組織の経営・戦略マネジメント(MBA と IT の融合)・実務/技術者それぞれの層において役割、現状の課題、今後の施策の方向性について打ち出した。

人材育成が見える事業として映るように、各層における教育・意識啓発などの施策を産学官連携を通して強化・推進する。

若年層における教育ニーヅとしての取り込み

中小企業へのセキュリティニーヅ対応、経済インセンティブなど

参加者からの質問・意見など

- サイバーセキュリティによるエコシステムをどのレベルまで遂行するのか？
- サイバーセキュリティー協議会とは具体的にはどういったものか？(バーチャルセンター)
- 日本社会ではセキュリティー犯罪による事故が起きた際、犯罪者ではなく被害者を悪者扱いにする傾向がある。

- 事故分析のためのデータアクセスは法律、国家・組織制度による制約が存在するため、現実的には様々な壁にぶつかることが予想される。
- これまでの任務保障(米軍 Mission Assurance の語訳）から表現的に変化があるのはどういった経緯からか？
- 「国際社会の平和・安定及び我が国の安全保障」はどこが主幹として行っているのか？内閣情報調査室

人材育成取組方針について

- アメリカの取組みを参考にするとはどういうことか？
- ３段による取り組みは米国で主流なのか？
- 米国ではセキュリティ人材は計２９種類ある。これに対して日本では職種がどういうものかという説明がなく、人に着目して名前だけが先行するため、実際には何をやるのかがわからないというケースが多い。そこは日本企業の戦略的マネジメント層における現状の大きな課題として取り上げられている。
- Social Engineering や脆弱性は以前から存在しており、時を経るごとに進化・巧妙化し、脅威の拡大に手を貸しているため、グローバルレベルでのガバナンスに関わってくる。
- MPA のように経営と情報の融合を意図したツール・プログラムは日本の教育機関には今だに見られていないが現実的に開発可能か？
- 日本では経営はジェネラリスト型で情報・セキュリティ系は専門職人材と見られるのが一般的で、人材のキャリアパス多様性には日本の終身雇用制とアウトソーシングがに立ちはだかる。
- 日本では今のところ無法地帯ネットワークの擬似的環境を作る土壌がまだ出来上がっていない。サイバー攻撃に対するデータ収集・分析を日本国内の企業レベルで行えるようにすることは今後可能か？
- 海外事業を持つ企業は現地でデータ収集・分析を行うことは比較的容易である。国内では現状として難しいのが現実だが、稀に特例として許可が得られることもある。暗号や detection など特定のカテゴリーに絞り、自動車などの分野に限定した上で試験的に実施する企業は今後いくつか出てくると考えられる。