資料8

意見書

2018 年 7 月 25 日
日本電気株式会社
代表取締役会長
遠藤　信博

1. サイバーセキュリティ戦略(案)について

政府関係者、パブリックコメントをご提出頂いた個人や企業・団体の御努力により、サイバーセキュリティ戦略(案)がまとまりました。近年、IoT や AI 技術の急激な普及により、サイバー空間自体が大きな変貌を遂げようとしています。今回、こうしたサイバー空間を取り巻く環境変化を取り込み、さらなる日本の発展をめざすサイバーセキュリティ戦略を練れたと思っています。

さて今後、本サイバーセキュリティ戦略(案)の実現にあたり、最も重要なことは「戦略(案)のインプリテーション」です。具体的な実行内容、達成目標、実現時期を明確化するとともに、どの省庁が予算を確保しその実行に誰が責任を持つかを明確化し、全体調整と進捗を管理することが重要です。また、可能なものに関しては、数値目標を設け、その実現に向けての過程を細かくコントロールすることも必要だと思います。特に攻撃者は、しばしば防御側のすきまを狙ってきます。複数省庁・組織に渡るテーマの場合は、分界点に齟齬がないかの確認が大切だと思います。また今回、「空港」が 14 番目の重要インフラとして追加されましたが、同様に「重要指定されていないが攻撃時の被害が大きなインフラ」のリスクが過小評価されることを懸念しており、攻撃組織の動向を把握し、状況に応じた対策強化ができる体制も必要だと思います。

また、現在政府で検討中のデジタル・ガバメントでは、共通のデジタル・プラットフォームを活用し DX(デジタルトランスフォーメーション)の実現をめざすことになりますが、セキュリティ要件に関しても共通化し、各省庁において共通レベルのセキュリティを確保できることが望ましいと思います。

今後の 3 年という期間内には、東京オリンピック・パラリンピックの開催が控え

ており、今まで日本政府が取り組んできた数々のセキュリティ施策が、実際の場で効果が試される期間になると思います。今までの戦略(案)を大幅に上回るレベルで、あらゆる視点から戦略(案)の効果検証を行う必要があると思います。

2. 将来に向けての布石

サイバーセキュリティ戦略(案)では、3 年程度の期間をターゲットに戦略を作成していますが、研究開発・人材育成など成果を見るまでにさらに長い期間を要するテーマもあります。こういったテーマに関しては、各国の動きとも協調しながら、長期的視野のもと、戦略(案)を実行することに期待したいと思います。

特に世界中で提起されている「セキュリティ人材不足」というテーマに関しては、短期間で成果が出せるような課題ではありません。高度人材・一般人材の両方で、十分な質と量を達成することが必要であり、防御に必要なレベルは攻撃側との微妙なバランスで決まるものだと思います。また、目標達成には時間がかかると思いますが、日本の教育制度(初等・中等・高等・生涯教育)やワークスタイルの変革とも密接に連携しながら、改善を計って行く必要があります。

同時に、人材だけではカバーできない部分に関しては、将来に向けて、人工知能(AI)の活用に関する研究開発と実用化推進を着実に行うことが重要です。さらには、将来確実に訪れる IoT と AI が融合した社会を前提にし、AI によるリアルタイム処理とリアルタイム処理が巻き起こす未経験の事象にも対応可能な「サイバーセキュリティ技術」の在り様を深く考える必要があると言えます。

以上