資料９

意見書

2015 年 2 月 10 日
日本電気株式会社
代表取締役執行役員社長
遠藤　信博

1. サイバーセキュリティ戦略本部の発足について

先月のサイバーセキュリティ戦略本部ならびに内閣サイバーセキュリティセンターの発足は、日本のサイバーセキュリティ対策を前進させていく上で大きな一歩であったと思います。今後、サイバーセキュリティ戦略本部を核に、緊急の事態やサイバーセキュリティ情勢の変化にダイナミックに対応できるよう、さらなる努力を続けることが肝要だと思います。

新しいサイバーセキュリティ戦略本部が達成すべきテーマは多岐にわたり、すべてを一挙に解決できるわけではありません。優先度を設定し、段階的にセキュリティを強化していくことも重要となります。特に人材育成、高度な技術の開発などの中・長期的課題に関しては、進むべき方向性を明確に示し、年度毎に設定した目標を着実に達成していくこと、定期的に方向性の見直しを行うことが大切です。

2. サイバー空間の情勢

さて現在、サイバーセキュリティ関係の記事を見ない日が無いほど「サイバー攻撃」は頻繁に発生しています。さらに昨今の国際情勢の悪化は、今後のサイバー空間の安全性に暗雲を漂わせる原因となっています。サイバー攻撃の背景に国家の関連が疑われるケースもあり、日本政府が中心となって攻撃の情報収集と解析・対策に当らなければ、対応が難しい状況になりつつあります。

こうした中、サイバー攻撃情報を共有することの重要性を再認識すべきと考えます。民間の企業では、部分的な情報の収集・把握は可能でも、包括的な情報の解析・分析は困難です。政府機関や民間の機関が収集した情報を、リアルタイムに近い形で官民の組織で共有し、それに対して日本全体でダイナミックな防御体制を敷く必要があります。今までも、経産省が主導する「J-CSIP(サイバー情報共有イニシアティブ)」や警察庁が主導する「CCI(サイバーインテリジェンス情報共有ネットワーク)」、あるいは官と民と接点となっている「官民ボード」や「JC3(日本サイバー犯罪対策センター)」、各種業界のセプターや業界団体など情報共有の核が存在し活発な活動を行ってきていますが、これらがもつ情報やノウハウ・分析結果を、サイバーセキュリティ戦略本部や内閣サイバーセキュリティセンターで統括的に把握し、交流を活性化させる必要があります。また、上記のような地道なサイバーセキュリティ活動のより一層の充実と範囲の拡大を計ることも重要です。

3. 国際化する日本

2020 年の東京オリンピック・パラリンピックを待つまでもなく、2016 年の主要国首脳会議（サミット）、2019 年のラグビーワールドカップなど、国際的なイベントが日本で相次いで開催されます。これらのイベントでは、多くの外国人の方が来日されると同時に、これらのイベントに狙いを定めた大規模なサイバー攻撃が発生する確率が高いです。日本の政府や産業界としては、総力を挙げてこれらの攻撃に適確に対応するとともに、これにより日本のサイバーセキュリティの技術レベルの高さを内外に示す事が重要です。

これらのイベントにおいては、イベントの期間だけセキュリティ監視・防御を強化しても、執拗な攻撃を防ぐことは困難です。攻撃者は、何年も前から、徹底した調査を行い、隙があれば関係するシステムや政府機関や関連企業、あるいは使用されるであろう IoT 機器にバックドアを仕込もうと仕掛けてきます。これらに対抗するためには、一日も早くソフトウェア開発業界に「セキュアな設計・開発を行う習慣」を根付かせ、一定レベル以上のソフトウェア製品・システムを日本に定着させていくことが重要です。こうした民間企業の取り組みに対してインセンティブを検討する必要もあります。また、新たに見つかった脆弱性に対しては、速やかに周知や対応ができる体制を敷く必要があります。さらにこの機会に、我々の日常生活を支える IT インフラに関しても、サイバー攻撃を受けることを前提としたセキュリティの見直しが必要と思います。交通、電力、ガス、金融などの分野では、サイバー攻撃対応力のレビュー(ペネトレーションテスト・演習等)を繰り返し行い、短い周期で改善スパイラルを回すことにより、実効性の高い防御力を獲得する必要があると思います。

このような施策を実現するためには、政府や地方公共団体に関しては、既存のガイドラインに基づいて導入するシステムのセキュリティレベルを段階的に向上させていくことが必要です。また、重要インフラ事業者等に関しては、セキュリティ向上のために、ガイドライン類の適用方向性を定義するフレームワークの整備に取り組むことが必要だと思います。同時に、内閣サイバーセキュリティセンターでは、稼働しているシステムのセキュリティ状況を常に把握し、セキュリティ対策の陳腐化や形骸化を監視することが重要です。

特に、アジアの国々は日本の各種セキュリティ施策や技術に強い関心を示し、期待をしてくれています。これらの国々の模範となり、強いリーダーシップを発揮することができるよう、世界トップレベルのセキュリティで守られた国家を実現させる必要があります。

4. 人材育成

日本ではサイバーセキュリティ人材が「量」と「質」の両面で大幅に不足しています。

まず、「量」という観点では、すでに社会で活躍している IT 人材(システムエンジニアやソフトウェア開発者)にセキュリティの専門知識を教育することで、一定数の人材確保が可能です。足りない部分に関しては、社会人予備軍である大学・大学院生への専門的教育実施や、今までセキュリティ分野では活躍の場が少なかった女性の登用も効果的です。

このためには、単に教育を行うだけではなく、受け入れ側であるセキュリティ業界の魅力を向上させていく取組みも必要だと思います。

次に人材の「質」に関してですが、これは一朝一夕での解決が難しく、時間をかけた育成が不可欠です。そのためには、中学・高校レベルから優秀な学生の素質を伸ばす教育を行い、さらに大学では優秀な学生を集め、世界に通用するトップガンに育てるような教育が必要と考えます。さらには、これらの人材を引き受ける産業界や教育界では、長期に渡る活躍の場を提供・保証する必要があります。これらに産学官が協力して取り組んでいくことが重要であると思います。

以　上