資料7

有識者構成員意見

情報セキュリティ政策会議へのコメント

2014 年 7 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. 我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針

IoT(Internet of Things)技術により、すべてのモノがインターネットに接続される時代は間もなく訪れます。一方、この「IoT」が実現された環境では、すべてのモノがサイバー攻撃の対象にさらされる可能性を秘めています。この社会では、攻撃者・犯罪者は「モノ」の本来の機能の一部を攻撃するだけで、社会を混乱させることが可能となります。我々は安全・安心な生活を維持するため、これらの攻撃にリアルタイムに対応できる「ダイナミックな体制」と「止まらない社会システム」を構築する必要があります。

このように、来たるべき IoT 社会に向けて、サイバーセキュリティの維持、サイバーセキュリティ技術の確立は、官民を挙げて取り組むべき国家の重要な課題です。今回の推進体制の機能強化では、喫緊の課題である高度サイバー攻撃の対処に加えて、法的権限が担保されたより実効性のある司令塔としての役割をめざしており、機能強化を迅速かつ確実に成し遂げる必要があると思います。

2. 情報セキュリティ研究開発戦略

本戦略では、一般的にはまだ知名度が低い「制御システムのセキュリティ」、地道な継続研究が必要な「コア技術の保持」等、基本的なセキュリティ対策技術に対しても配慮された内容となっています。さらに、今後の課題である「IoT」 や 「次世代ネットワーク」、「パーソナルデータの利活用」がリストアップされており、重点化された戦略となっています。

現在、政府や企業において最大の脅威となっているのは、「高度サイバー攻撃」です。高度なサイバー攻撃に対応するためには、攻撃者の手の内を知ることが重要です。すなわち、「マルウェア」や「脆弱性」の解析の研究を進め、それらの知見に基づいて「対策製品の開発」まで推し進める施策が必要です。本戦略においても、「攻撃情報の共有」「研究者への検体の提供」など、現場のセキュリティ研究者が必要としている施策が盛り込まれました。まだ日本では、マルウェア等の研究者・研究活動は多くはありませんが、これらの実現によって研究が活性化され、対策が加速されると思います。

そして、本戦略の加速がサイバーセキュリティ産業の発展につながるようさらなる検討が必要だと思います。

3. サイバーセキュリティ政策に係る年次報告(2013 年度)

2013 年は前年に比べ、政府機関が受ける脅威の件数が約 5 倍に、インターネットバンキングの不正送金が 14 倍に激増しています。攻撃が集中している分野では、個別の対策強化を検討する必要があると思います。また、高度サイバー攻撃の質の変化も報告されて

いますが、高度サイバー攻撃に関しては、単に数量だけの分析に終わらせず、攻撃に使用されたマルウェア、攻撃手法、攻撃の持続期間、攻撃者の特徴等に関して、省庁横断的に詳細な分析を行う必要があります。

4. サイバーセキュリティ 2014

昨年度検討した「サイバーセキュリティ戦略」に最新のサイバーセキュリティの動向も加味し、バランスが取れた年次計画となっていると思います。東京オリンピック・パラリンピックで世界の注目を集めている中、2020 年に向けた良いスタートを切る必要があります。特に、「世界を率先するサイバー空間」に関しては、二国間、多国間の協議、諸外国との連携を通じて、日本がリーダーシップをとれるよう、政府を挙げたバックアップ体制が必要です。そのためには、NISC の機能強化が最低限必要であることは言うまでもないと思います。

5. 高度サイバー攻撃対処のための取組等

高度サイバー攻撃を防御するためには、マルウェアや URL リンクを使用した標的型メール攻撃を、評価環境で動作させる等の手法で確実に検知し内部ネットワークへの新たな侵入を防御する必要があります。同時に、すでに内部ネットワークに侵入を許している場合には、探索活動、窃取活動等の侵入者の僅かな活動の特徴やツールの使用を捉えて、発見駆除することが必要です。

高度サイバー攻撃は短期間で攻撃手法が進化する傾向が顕著に見られ、官民に共通した課題となっていることから、本取組みで政府が得た攻撃手法に関する情報、マルウェアに関する情報を可能な範囲で民間組織と共有し、フィードバックを受けることが必要と思います。

同時に、先ほども述べました社会インフラの機能を麻痺させるような DDoS 攻撃、あるいは破壊型攻撃、ランサムウェアも視野に入れた対処法の確立が必要と思います。

以上