資料2

有識者構成員意見

① 小野寺構成員意見

情報セキュリティ政策会議へのコメント

2013年3月26日

小野寺　正

１．環境変化

従来の情報セキュリティは、主にオープン系（The Internet）における脅威が主でした（DoS 攻撃、フィッシング詐欺等)。しかし最近は、従来比較的安全とみられていたクローズド系（イントラネット、制御系）への攻撃が目立つようになってきました。標的型攻撃メールやマルウェアなどは The Internet を経由してクローズド系への入り口を探し出し、機密情報や重要インフラにアクセスします。このような環境変化をもう少し明確に記載すべきと考えます。

２．重要インフラにおけるセキュリティ強化の具体的な推進

重要インフラを狙った攻撃が極めて増加しています。これまで、Stuxnet(2010)、Duqu（2011)、Flame(2012)、Shamoon(2012)などのマルウェアによる重要インフラ攻撃が世界規模で見られており、昨今では、上記の Shamoon と酷似するマルウェアを用いた韓国への重要インフラ攻撃があったところです。

今回の「新たな情報セキュリティ戦略の方向性について」においても、重要インフラ防護に向けた取り組みの重要性は取り上げられており、「政府機関等における対策に準じた取組」が必要とされています。しかしながら、以前に策定された政府の取り組みにおいても同様な宣言があったものの、具体的な重要インフラ防護のための方向性が明示されていないため、本取り組みに対する明確な成果が見えていない状況にあるように思えます。

このためには、これまでの活動に加えて、１）海外の重要インフラ攻撃成功事例の徹底分析、２）SCADA や AMI(Advanced Metering Infrastructure)などの重要インフラ独特の環境を想定した評価実証環境の構築など、重要インフラに特化した具体的な技術検討が必要になっていると考えます。セプターカウンシル、及び各セプターにおける本課題の共有に加え、関連する研究機関との強く連携することにより、早急に強靭な重要インフラ防御に向けた対応を具体的に強化すべきです。

３．情報通信関連事業者等による自浄的・自立的な役割について

ナショナル・セキュリティの確保、増進等のためこれまで、政府機関、重

要インフラ事業者、企業、国民の四領域に向け対策を検討してきていますが、今般、役割主体として「情報通信関連事業者等」が追加で言及されています。

従来から情報通信は重要インフラとして位置づけられており、セプターカウンシルの活動においても先導的な役割を担ってきました。

基本的な方針にも示されているように、「社会的な立場に応じた役割を発揮」すること、すなわち「サイバー空間」の全てのステークホルダーが自ら行動することが重要です。

「情報通信関連事業者等」を別掲した場合、「情報通信関連事業者等」が「サイバー空間」を守ってくれるから大丈夫、という誤った情報として捕らえられることを危惧します。

これまでも「情報通信関連事業者等」は安心・安全なネットワークの提供に努力をしてきました。しかし、The Internet は完全なオープン系・分散系であり、情報通信関連事業者といえども The Internet 全体を見られるわけではありません。まして現在問題となっている重要インフラへの攻撃は閉鎖系に対する攻撃であり、通常は情報通信事業者も与り知らない部分です。

「情報通信関連事業者等」を別掲することには多くの問題を含んでいます。

４．リスクベースによる対応のためのリスク分析について

リスクの分析を行い、想定できるリスクに基づく優先度を精査し、適切な対策を講じることは重要です。現状のリスク算定では、想定脅威、既存の脆弱性、資産価値、などを組み合わせることにより、影響度などの「リスク」の分析・算定を実施しますが、算定されるリスク値は「想定脅威」に強く影響されます。リスク分析以前に、「脅威分析」を行う必要があります。

脅威分析を実施するための具体的な施策、たとえば、初期の攻撃挙動検知、攻撃情報の早期共有体制の構築、攻撃の早期解析技術の高度化などを進める必要があります。