

「電気通信事業におけるサイバー攻撃への適正な在り方に関する研究会」

ワーキンググループ第1回議事要旨

1. 日 時：平成25年12月11日(水)14:00～16:00
2. 場 所：総務省8階共用801会議室
3. 出席者：
 - (1) 構成員
穴戸主査、衛藤構成員、木村構成員、小山構成員、齋藤構成員、丸橋構成員、村主構成員、森構成員
 - (2) 総務省
玉田消費者行政課長、山碕情報セキュリティ対策室長、藤波消費者行政課企画官、村上情報セキュリティ対策室調査官、森里消費者行政課課長補佐、平松情報セキュリティ対策室課長補佐
4. 議事要旨：
 - (1) 開会
 - (2) 議事
 - ① 開催要綱、議事の運営について
本ワーキンググループの開催要綱及び議事の取扱いについて了承され、開催要綱に則り森構成員が主査代理に選任された。
 - ② 事務局説明
総務省から資料2に基づき、サイバー攻撃への対処に関する現状における課題と本ワーキンググループにおける検討の方向性案について説明が行われ、質疑応答が行われた。
 - ③ 外部有識者によるプレゼンテーション
外部有識者を招き、鶴飼氏(株式会社FFRI、セキュリティベンダとしての現状と課題について)、岡本氏(トレンドマイクロ株式会社、最近の攻撃の脅威動向について)、高橋氏(日本マイクロソフト株式会社、当社における取組について)及び針生氏(NTTセキュアプラットフォーム研究所、当研究所における悪性サイトの検知技術の研究開発状況について)からそれぞれプレゼンテーションが行われた。
 - ④ 質疑応答
事務局説明及び外部有識者のプレゼンテーションを踏まえ、外部有識者と構成員の間で質疑応答が行われた。主なやり取りは以下の通り。
 - ・ セキュリティベンダとして、通信事業者の取組が事業の障害になることがあるか。
⇒セキュリティベンダとしても可能なことと不可能なことがあるので、規模が必要となるもの等、通信事業者や国と協力して進められればと考えている。

- ・ 車やM2M等新しい領域についてのセキュリティが課題になっているが対策はあるか。
⇒PC・サーバ以外の領域におけるセキュリティ対策が大きく取り沙汰されるようになってきているが、根本的なセキュリティ対策を実施することと攻撃のコストを上げることが重要。
- ・ 今の通信の秘密は人間同士の通信が前提であり、M2Mのように機械同士が通信する際、通信の秘密はどう考えるべきか。
⇒通信の中を見ないこととセキュリティ対策をすることが対極に近いところがあるので、前提として、日本としてどういうインターネットを作るかということを考えていく必要がある。
- ・ 次の攻撃手法を明らかにするのは難しいが、次に狙われそうな所を防御するという考え方があると思うがどうか。
⇒防御しても一度攻撃のベクトルが見つかる(攻撃者の)研究が早いことから、新しい攻撃手法に対する安全性を高めるというアプローチに加えて、エンド・ツー・エンドトラストのような、使っている人間、使っているコンピューター、使っているネットワーク、これらが全てトラस्टッドであると確認できる環境をつくっていくというアプローチも必要。
- ・ ぜい弱性を突いたウェブサイト改ざんの攻撃について、攻撃側と防御側でいちごっこになる印象がある。大きなテーマで通信事業者として何かやった方が良く考えるがどうか。
⇒これも、通信は単なる土管でいいのか、という議論と結びつく。通信事業者が単なる土管の役割から脱却し、攻撃するコストが上がるような環境を構築したとしても、ぜい弱性を突いた攻撃を止めることについて、是非が難しい。通信の秘密との関係では、構成要件も含めて議論が必要。
⇒今までは、通信事業者にとって、サービスを提供するうえでやむを得ず実施しなければならない、という観点からの議論が中心であったが、今回の議論は、ユーザにとってのリスクが中心であると思えるので、ユーザからの社会的要請と、事業者側としてリスクとして考えていることとの架け橋を作ってうまく整理できればよいと思う。
- ・ 今後の検討にあたっては、通信の秘密の侵害に関する違法性阻却事由について、従来の考え方を踏襲しつつ、特に正当業務行為の解釈について整理していく余地があると思う。

(3) 閉会

今回の日程などについて、事務局から説明が行われた。

以上