

「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2回議事要旨

1. 日 時：平成 26 年 1 月 30 日(木)13:00～14:30
2. 場 所：合同庁舎4号館共用 108 会議室
3. 出席者：
 - (1) 構成員
穴戸主査、森主査代理、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
 - (2) 総務省
玉田消費者行政課長、赤阪情報セキュリティ対策室長、藤波消費者行政課企画官、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 検討事項に対する整理状況について
前回ワーキンググループにおいて検討すべきこととされたものについて、事業者構成員より資料1、事務局より資料2にそれぞれ基づき説明が行われた。事業者構成員からは、C&Cサーバに蓄積された情報をもとにしたマルウェア感染の更なる駆除、DNSAmPという新たな DDoS 攻撃の防止、SMTP認証の情報を悪用したスパムメールへの対処について法的整理の検討状況の説明が行われ、サイバー攻撃の未然の防止及び被害の拡大防止については引き続き検討する旨の説明があった。事務局からは、マルウェア配布サイトへのアクセスに対する注意喚起における有効な同意の考え方について説明が行われた。最後に、質疑応答が行われた。
 - ② 質疑応答
事業者構成員及び事務局説明を踏まえ、質疑応答が行われた。主なやり取りは以下のとおり。
 - ・ 諸問題研での整理においては、「事前の包括同意は将来の事実に対する予測に基づくため対象・範囲が不明確となる」とされているが、オプトアウト等を条件に約款同意による事前の包括同意を認めることは、この課題に対してよい解決方法と思われる。ただし、それにはオプトアウトに関する周知がきっちり行われることが必要。
 - ・ ACTIVE の中で利用者が自らツールバー等のソフトウェアを端末にインストールして、端末上で対応するものについては、ISP の方でオプトアウトさせることはできない。
⇒そのような場合は、そもそも通信の秘密の問題ではない上に、利用者が自ら端末にソフトウェアをインストールしており、そのことをもって同意していると考えられる。

- ・ 契約約款に基づく同意の考え方については、ISPがネットワーク側で、マルウェア配布サイトへのアクセスを検知・遮断することを可能にする整理だと思うが、現実にはこのようなことができる事業者は限られていると思われる。
⇒ISPによって状況は様々だと思うので、現状全てのISPが対応可能かというところではないとも思う。契約約款に基づく同意により、マルウェア配布サイトへのアクセスに対する注意喚起を行うに当たっては、どういう実装の形になるかは今後議論したい。
- ⇒これまで、このような考え方がされていなかったため、検討すらできていない事業者もあると思うが、この考え方が示されたことによって、これから考えていく事業者もいると思う。
- ・ SMTP認証の情報を悪用したスパムメールについて、一時停止の対象となる SMTP 認証の ID であるか否かを判断するに当たって、認証の際に使用されたIPアドレス数や送信されたメール数の閾値等について、何らかの目安はあるか。
⇒ISPによっても、また利用者によっても態様が異なるため、一般的な目安を立てるのは難しい。

(3) 閉会

次回の日程・議題などについて、事務局から説明が行われた。

以上