

レジデンシャルプロキシ対策アライアンス(第1回) 議事要旨

1. 日 時 令和8年9月7日(月)10:00～11:45

2. 場 所 総務省会議室(Web 会議併用)

3. 出席者

【構成員】

星座長、吉岡副座長、井上構成員、久保構成員、小山構成員、渡辺構成員、櫻澤構成員、
加治川構成員、任田構成員、大石構成員、井浦構成員、松本構成員、儀間構成員、萩原構成員

【オブザーバー】

内閣官房国家サイバー統括室参事官、
総務省情報流通行政局放送業務課配信サービス事業室、
経済産業省商務情報政策局サイバーセキュリティ課

【警察庁】

(サイバー警察局サイバー企画課)
根本サイバー企画官

【総務省】

(サイバーセキュリティ統括官室)
道方サイバーセキュリティ統括官付参事官(政策担当)

4. 配布資料

資料1-1 「レジデンシャルプロキシ対策アライアンス」開催要綱

資料1-2 警察庁の取組(警察庁)(一部非公開)

資料1-3 総務省の取組(総務省)(一部非公開)

資料1-4 レジデンシャルプロキシ対策アライアンス第1回会合(ICT-ISAC)(一部非公開)

資料1-5 レジデンシャルプロキシの観測・分析と対策に向けた取組み(NICT)(一部非公開)

資料1-6 レジデンシャルプロキシとサイバー犯罪(JC3)(一部非公開)

資料1-7 本アライアンスの検討項目案(一部非公開)

資料1-8 今後のスケジュール

5. 議事概要

(1) 開会

(2) 議題

◆議題(1)「レジデンシャルプロキシ対策アライアンス」の設置について

資料1-1に基づいて事務局から説明が行われた。

◆議題(2)各関係者の取組

資料1-2に基づいて警察庁から、資料1-3に基づいて総務省から、資料1-4に基づいてICT-ISACから、資料1-5に基づいてNICTから、資料1-6に基づいてJC3からそれぞれ説明後、各関係者の説明を踏まえ、質疑応答が行われた。質疑応答での構成員による主な質問及び意見は以下のとおり。

- レジデンシャルプロキシを提供するサービスにおいて、正規のものと悪用目的のものを区別することは難しい。提供企業のプロフィールの有無、当該 IP アドレスや拠点に関する不正利用情報への対応姿勢、ソフトウェア提供時の機能説明の程度などに提供者の意図が表れ、判断の観点となるのではないかと。
- レジデンシャルプロキシを提供するサービスは多様であるが、不特定多数の利用者が利用できるサービスについては、悪用されることを前提として対策を検討すべきである。
- 利用者が認識しないままサイバー攻撃の踏み台とされている実態は大きな問題。利用者への個別警告等を行い、そのような状態を解消していく取組が必要。
- 電気通信事業者は被害申告に基づいて利用者への注意喚起等を実施することとなるため、レジデンシャルプロキシの製品名等が特定できれば利用者において対策しやすいと考える。一方、被害申告による利用者特定や注意喚起を行う場合は、その方法を慎重に検討すべきであり、調査手法の適切性や確度、再現性を公に示した上で当事者に行動変容を促すべきである。
- 悪用されるとの認識がある上で、当該サービスや製品を提供あるいは購入することが違法行為であるかについての基準は明確にしておくべきである。例えば、刑事的には、犯罪利用の蓋然性を高く認識していた場合には幫助犯として、民事的には提供者に重大な過失がある場合には被害を及ぼしたとして違法性を問える可能性がある。たとえ問えない場合でも警告というプロセスが求められるのではないかと。

- レジデンシャルプロキシを経由した不正アクセスがあった場合、不正アクセス行為自体に着目して警察は捜査するため、悪用の認識の上でのレジデンシャルプロキシの提供又は購入について、何をもって違法とするかの判断は難しく、個別ケースとして取り上げて判断していく必要がある。

◆議題(3) 検討項目及び今後のスケジュール

資料1-7及び1-8に基づいて事務局から説明が行われた。星座長から、資料の公開可能な範囲の検討についてのご提案後、資料1-7及び1-8を踏まえ、質疑応答が行われた。質疑応答での構成員による主な質問及び意見は以下のとおり。

- 注意喚起は根本対処とはならないが重要な手段である。
- 海外では関係者が対応(テイクダウン)してから利用者に通知している対応も行われていることから、根本的な対処のために、警察及び電気通信事業者がより積極的に連携していくことを検討すべきである。また、利用者の意識啓発のためには、経済産業省の JC-STAR といった製品側からのアプローチや、メーカー及び電気通信事業者の連名での発信といった取組が有効ではないか。
- 経済産業省のリコール製品検索や厚生労働省の公表事例を参考に、メーカーへの注意喚起とあわせて、悪用される可能性のある製品名やアプリ情報を国民へ発信することについて、事実確認を行った上で、発信内容等を本アライアンスとして検討していくべきである。

(3) 閉会

以上