Residential IP Proxy への対応の課題

2026/2/13 JANOG 57
STB経由不正アクセスとは？犯罪プロキシサービスの実態解説

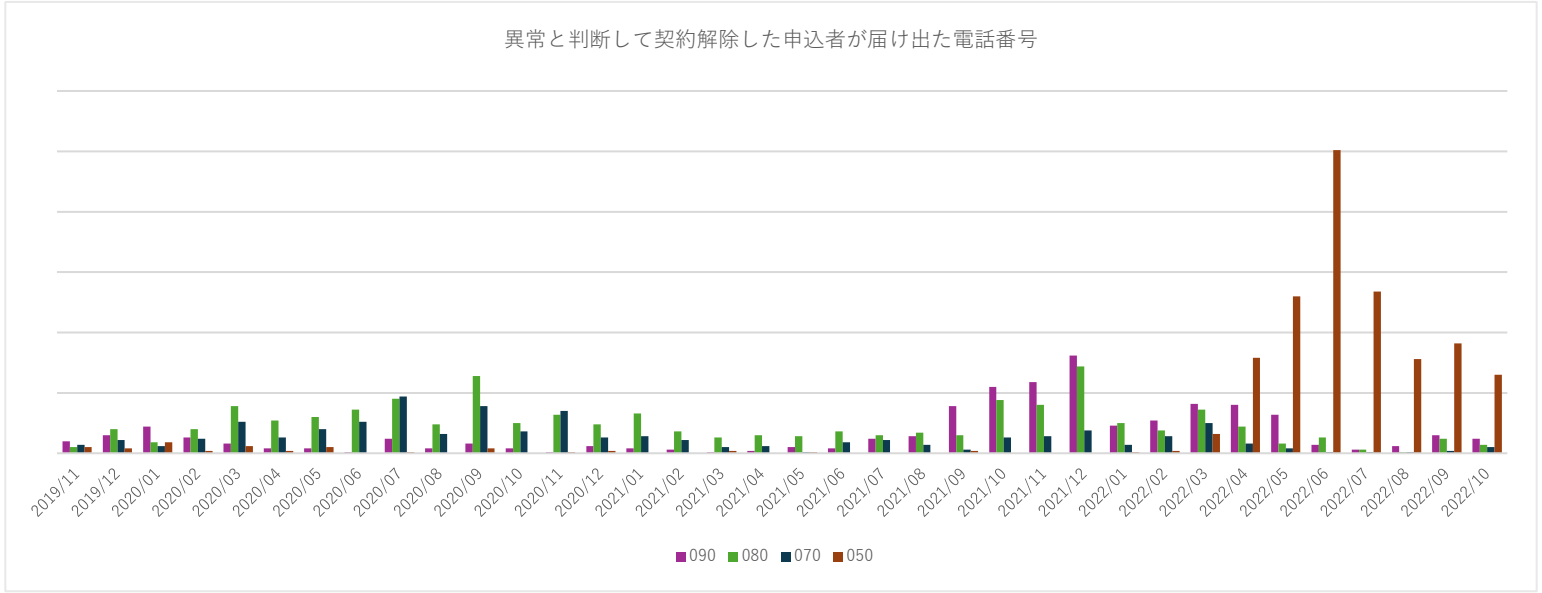
さくらインターネット株式会社 山下健一

RESIP Proxy経由アクティビティの観測例

1. RESIP Proxy経由で
   氏名・住所・電話番号が登録される
2. RESIP Proxy経由でクラウドサービスが契約される
3. RESIP Proxy経由で
   他人のクレジットカードが登録される
4. ダークマーケットに流通したSIMで？
   プロバイダの電話番号所有検証を突破する
5. クラウドインフラから
   フィッシング詐欺メールが送られる

※観測例はクラウド・ホスティングサービスの場合のよくある例です。
　オンラインサービス提供事業者のサービス形態により様々な類型があると思われます。

フィッシング詐欺師等が
契約時に持ち込んできた電話番号の例



※ 全てがRESIP Proxy経由で届けられた電話番号という訳ではありません。
半分前後？がRESIP Proxyらしきアドレス経由で届けられていた印象があります。

- 不正行為に利用される電話番号の傾向変化に注目
- 2020年はコロナで国際的な人の移動が制限されていた点に注目

対応する意味

- 「目に見える脅威」は「脅威の出口、表出したもの」、
  背後に犯罪インフラのサプライチェーンがある
- RESIP Proxyに対応することは
  「犯罪行為のサプライチェーンを絶つ」意味がある

  （たとえ断ち切れない場合でも、犯罪のコストを上昇させる意味はある）

ユーザーコミュニケーションの課題

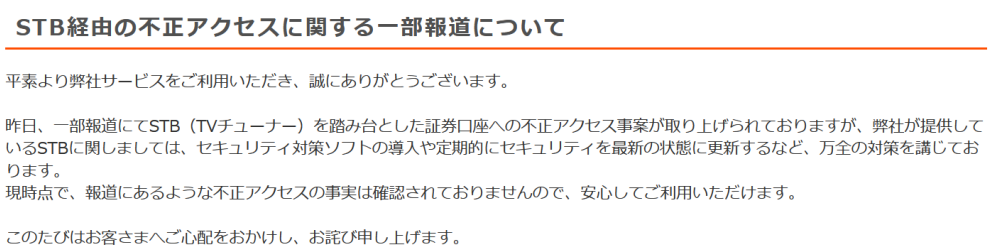
- どうやって連絡するのか、メールで連絡するのか

  ユーザーはプロバイダのメールなんて見ない
  （ユーザーは、ISPのメールボックスなんて見ない）
  （ユーザーはそもそもPCを見ているだろうか？　スマホで全部済ませてる）

- 電話はわかりにくい

  「予期しない内容を伝える電話」はコミュニケーションコストが高い
  イラスト等の視覚補助線が無いと伝わらない…郵便？

- 「セットトップボックス？」ユーザーには分からない



STB経由の不正アクセスに関する一部報道について

平素より弊社サービスをご利用いただき、誠にありがとうございます。

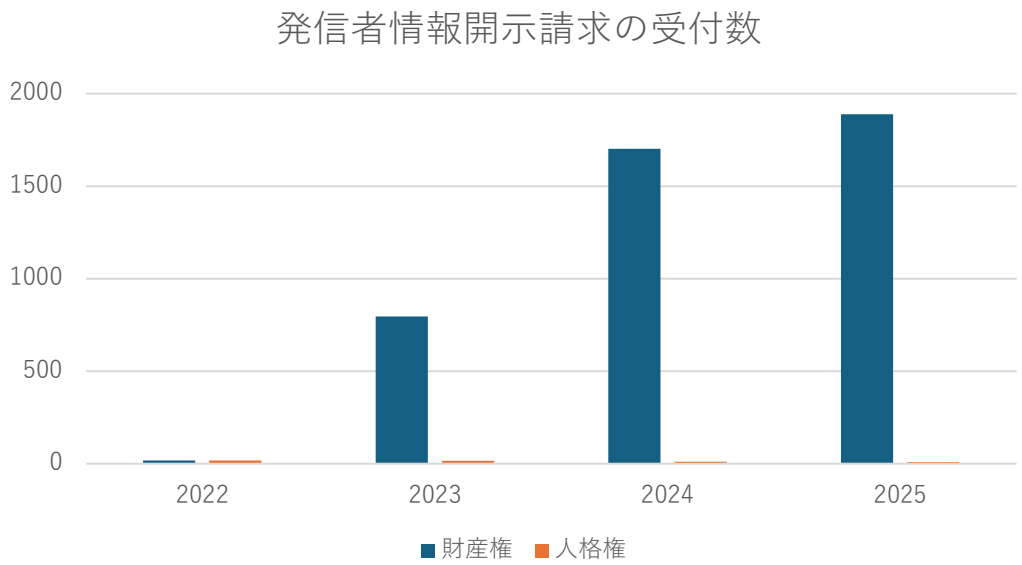
昨日、一部報道にてSTB（TVチューナー）を踏み台とした証券口座への不正アクセス事案が取り上げられておりますが、弊社が提供しているSTBに関しましては、セキュリティ対策ソフトの導入や定期的にセキュリティを最新の状態に更新するなど、万全の対策を講じております。
現時点で、報道にあるような不正アクセスの事実は確認されておりませんので、安心してご利用いただけます。

このたびはお客さまへご心配をおかけし、お詫び申し上げます。

← あるプロバイダさんがお出しになった
「お知らせ」の例(2025/9/25)

P2P発信者情報開示請求の増加

下グラフはあるプロバイダの発信者情報開示請求受付数



2022年 → 2023年 2,000%増！

2025年 財産権は人格権の200倍！

※「財産権」にはP2Pファイル交換等の著作権侵害の他、商標権侵害も含みます。

※「人格権」には名誉棄損（誹謗中傷）、プライバシー権侵害（氏名や写真の無断掲載）を含みます。

プロバイダーの対応コストの課題

- 「ユーザーの行動」はプロバイダーの責任の外

  現在プロバイダーが苦しんでいるのはP2Pファイル交換に関係する大量の発信者情報開示請求・非訟・訴訟

  IoTデバイスの異常の対応もプロバイダに期待される
  でもそのIoT／NWカメラ／STBは、売ったのも設置したのもプロバイダではない

  「ユーザーの行動」への対応がプロバイダに期待されがち
  誹謗中傷／海賊版の閲覧視聴／オンラインカジノ

- 技術的・組織構造的に
  「外部化できる対応」と「外部化できない対応」がある

  ログ（アクセスログ）とユーザーアカウント・契約の突き合わせも大変、
  CGN/CGNATが入ってる

RESIP Proxy固有のテクニカルな課題

- どのように「これは異常だ」と判定するのか

  検出申告や被害申告を信頼するのか？　誰がオーソライズするのか？
  検出の証跡は取れるだろうか？

- どのように「異常を再現確認可能にする」のか

  ユーザーに対する初動をISPが取る場合「＊＊から聞いたんです」は理由にならない。
  それではISP自身で再現確認できるようにする必要がある
  …でも再現確認できるだろうか？　誰が再現確認コストを払うのだろうか？

- 異常が確認可能であるとして、「通信の秘密」との整合性は？

  「確認する」ことは通信の秘密の侵害に当たらないか？

再発防止？

対応する傍から新規に問題発生していたらどうしようもない

- セキュリティ要件適合評価及びラベリング制度（JC-STAR）？
- 電気通信事業法？

電気通信事業法　第五十二条

電気通信事業者は、利用者から端末設備をその電気通信回線設備に接続すべき旨の請求を受けたときは、その接続が総務省令で定める技術基準に適合しない場合その他総務省令で定める場合を除き、その請求を拒むことができない。

- ブロッキングを行わない
  （消費者を不正VPNへ誘導するリスクを高める）

課題の整理

- ユーザーとのコミュニケーション課題をどう解決するか
- ISPの対応コストをどう扱うか
- RESIP Proxy固有のテクニカルな課題の解決
- 再発防止は？