



NICTにおける 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

久保 正樹

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
サイバー脅威分析室



レジデンシャルプロキシ全体像と課題

Technical Analysis

Measurement

2

課題2. 出口ノードの実装・制御基盤の把握

課題1. 国内出口ノードの継続観測・実態把握

① 攻撃者

(レジプロの利用者)



レジデンシャルプロキシサービスを使って目的のWebサービスへアクセス

サービスを利用

② レジデンシャルプロキシ事業者

管理・制御サーバ



制御・指示

中継サーバ



課題4. 出口ノードを介した悪用実態の解明

Abuse Analysis

③ 一般家庭のインターネット回線

(レジデンシャルプロキシの出口)

ホームゲートウェイ



出口IPアドレス
(例: 203.0.113.30)

インターネット



動画視聴機器

(proxywareが動作)



家庭 (LAN) 内の
他の機器



課題3. 出口ノード形成・拡大メカニズムの解明

Ecosystem / Recruitment Analysis

④ Webサービス

(金融、ECサイト、SNS)



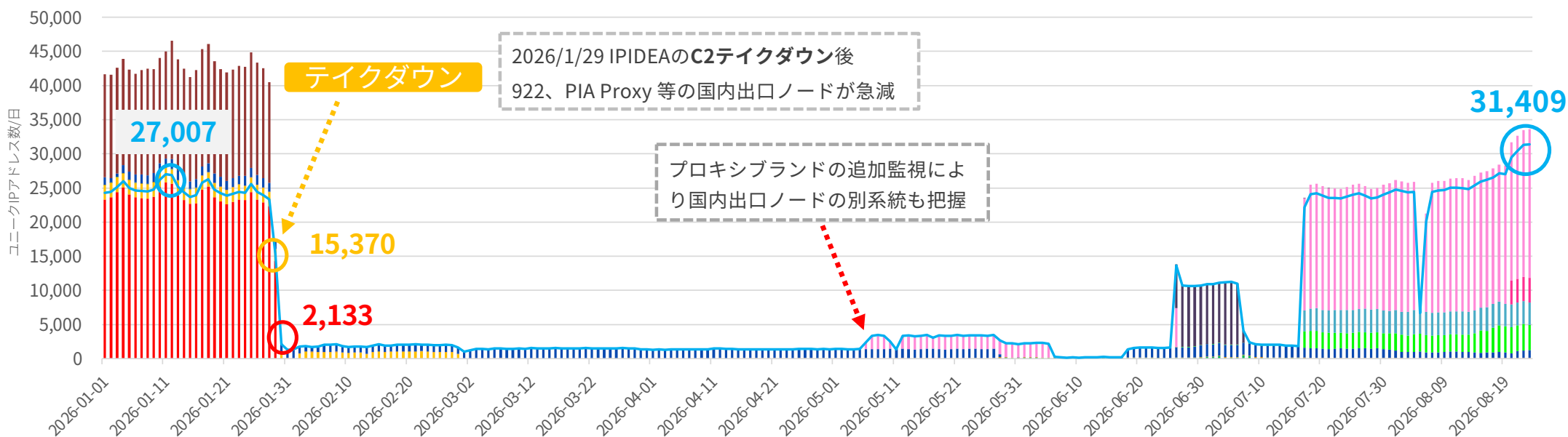
- アクセス元として家庭のIPアドレスが記録される
- 本来の通信元 (攻撃者) のIPアドレスは見えない



日本国内の出口ノード（2026年8月）

3

- ・ 月間59.6万IP、最大7.7万IP/日の出口ノードが存在（IPinfo社調査）
- ・ NICTでも約3万 IP/日の国内出口ノードを確認
- ・ 出口ノードは日々増減・入れ替わる。継続観測が必要





国内レジプロ基盤の長期変化と構造把握

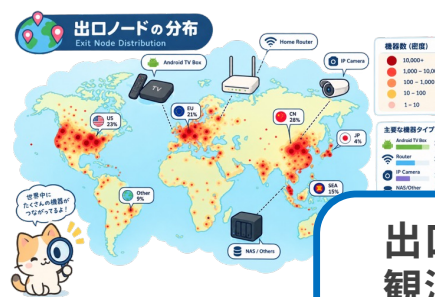
課題1

4

① 規模、分布の把握

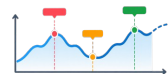
【調査内容】

- 国内出口ノード数
- AS / ISP別分布（特定ISP・ASへの集中）
- 固定回線／モバイル回線等の回線種別
- 地域別分布
- ブランド別シェア
- ブランド間でのIP重複



出口ノード 観測データ

IP / AS・ISP / 回線 / ブランド



② 出口ノードの実態調査

【調査内容】

- rDNS hostname等から組織・ネットワークを特定
- 大学・企業・研究機関など、連絡可能な出口ノードを抽出
- 当該組織やISPと連携し、現地調査の協力を依頼**
 - ✓ 端末（OS / ベンダ / モデル）
 - ✓ どのproxywareが導入されたか

IPアドレス

ホスト名

組織名

③ IoTボットネットとの重複、 関連性分析

【調査内容】

- ボットかつレジプロになっているIPの割合
- 特定ボットネットとの重複

【既存研究】

- Google：IPIDEAが proxyware/SDK/BadBox2.0、Aisuru、Kimwolf等との関連を報告
- Bitsight：IPIDEAテイクダウン前、Vo1d感染端末がIPIDEAの出口ノードとして機能



④ インフラの変動、再編

【調査内容】

- ブランドの出現・消失
- ブランド間の IP pool 共有
- ブランド/事業者間の関連性
- テイクダウン・ブロッキング後の影響・回復状況

**継続観測することで、実態や構造変化を把握
→優先度に基づく対応に繋げる**



- ## ・ 悪用実態の分類・定量化生成

✓悪用トレンド（類型、頻度、宛先、時間的傾向）

エミュレータによるProxy通信の復号・監視



NICTのレジプロ分析・対策に向けた活動方針

14

- 以下の4課題を軸にレジプロの実態把握を進める
 - ✓ 国内出口ノードの継続観測・実態把握
 - ✓ 出口ノードの実装・制御基盤の解明
 - ✓ 出口ノード形成・拡大メカニズムの把握
 - ✓ 出口ノードを介した悪用実態の解明
- これらを横断的に組み合わせ、レジプロエコシステム全体を継続的に分析できるCapabilityを構築
- ISP、警察、ベンダとの連携を通じ、注意喚起、サプライチェーンへのアプローチ、テイクダウン/ブロッキング等の対策検討、効果検証につなげる