JPOPF-ST

インターネット番号資源
ホットトピックス

2025/11/19

谷崎文義/JPOPF-ST

この発表では…

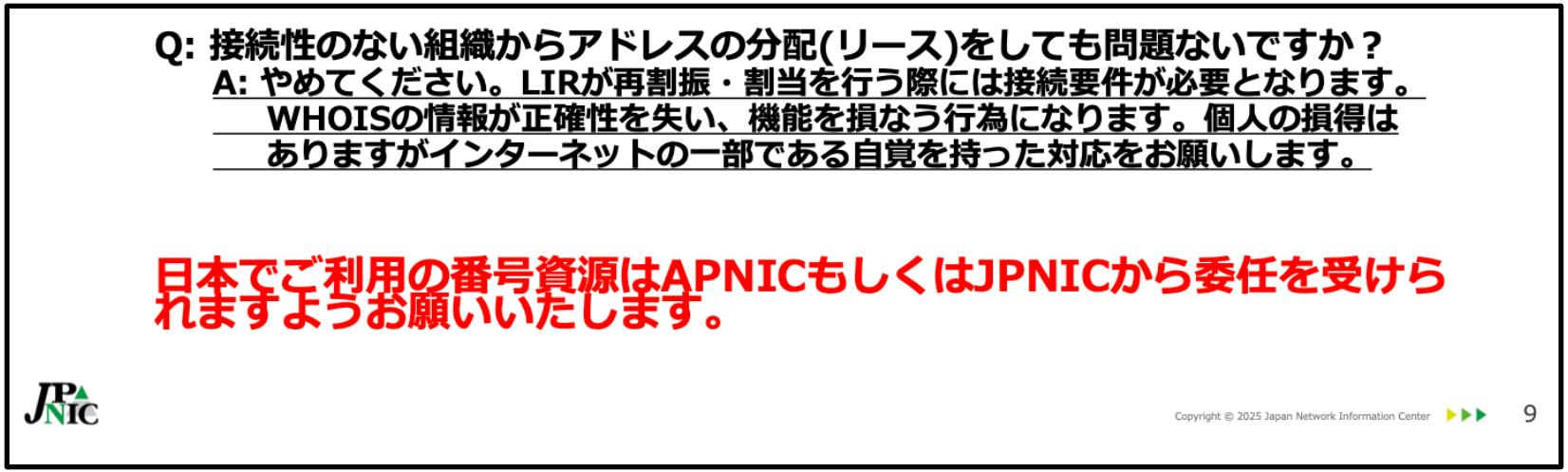
- インターネットに関する話題のうち、主に番号資源とポリシーに関わるものやその周辺を話題として取り上げます。
- キーワード
  - IPアドレス、AS番号
  - インターネットガバナンス
    - スプリンターネット、インターネットシャットダウン
  - その他興味深い話題
- ポイントは…
  - (できるだけ)旬な話題
  - ちょっと違った切り口
    - 個人的な意見や私見がたくさん
    - ある意味、**ヤジウマ**的な視点
  - 短くお話しします

論文紹介『IPv4リース市場における不正利用の調査』-1-

- 『From Scarcity to Opportunity: Examining Abuse of the IPv4 Leasing Market』
  - 直訳：不足から機会へ：IPv4リース市場における不正利用の調査
  - https://www.caida.org/catalog/papers/2025_from_scarcity_opportunity/from_scarcity_opportunity.pdf
- IPv4アドレスの枯渇後に台頭してきた**IPアドレスリース市場**と、それが**インターネットセキュリティに与える影響**を分析
  - 通常のIPv4アドレスとリースされているIPv4アドレスの『**汚れ具合**』を比較
- 著者
  - トゥウェンテ大学：Bernhard Degen, Raffaele Sommese, Mattijs Jonker, Roland van Rijswijk-Deij
  - **CAIDA**：Ben Du, Ricky K. P. Mok, kc claffy
- CAIDA（Center for Applied Internet Data Analysis）について
  - 所在地：カリフォルニア大学サンディエゴ校 サンディエゴ・スーパーコンピューターセンター
  - ミッションステートメント
    - インターネットのインフラストラクチャ、動作、使用状況、進化に関する巨視的な洞察を提供します。
    - データを取得、分析し、(必要に応じて)共有できる協力的な環境を育成する。
    - インターネット科学の分野の完全性を向上させる
    - 科学、技術、通信の公共政策に情報を提供します。
  - https://www.caida.org/

具体的な話の前に…

- **注意：これから論文の内容を紹介しますが、詳細は原文を参照してください！**
- **JPNICではIPアドレスのリースは禁止されています！**



JPOPM 48：資源管理の基礎知識～IPアドレス分配とポリシー～ (中川 香基/JPNIC)
https://www.jpopf.net/JPOPM48Program

論文紹介『IPv4リース市場における不正利用の調査』-2-

- 背景
- IPv4アドレス枯渇→IPv4アドレス市場の出現
  - 2024年には6,184件を超える移転があり、30.2Mのアドレスが取引された
  - IPブローカーが取引を仲介
- 昨今は**IPv4アドレスリースが普及**
  - リースは、高額な初期投資なしに規模を拡大したい組織にとって、費用対効果の高い代替手段を事実上提供
  - **リース期間は最短1ヶ月から存在**
- IPv4アドレスリースはセキュリティ的な課題を抱えている
  - **リースはWHOISに実際の利用者の詳細が記録されない**ため、インターネットの透明性を低下させ、**不正利用の苦情対応を困難**
    - IPアドレスリースとAbuseの現状 ～事例を通じた課題共有と調整への提言～
      - 中井 尚子(JPCERT/CC) / JPOPM48
    - https://www.jpopf.net/JPOPM48Program?action=AttachFile&do=view&target=JPOPM48_JPCERT_public.pdf
  - IPブロックリストなどのセキュリティ対策を回避するため、**異なるアドレス間を迅速にローテーション**している？？
  - 現在、5つのRIRのいずれも、ポリシーにおいてIPリースを**明示的に許可も禁止もしていない**

論文紹介『IPv4リース市場における不正利用の調査』-3-

- 元になったデータは？
- IPリース・マーケットデータ
  - 2024年12月21日から2025年3月12日までの期間、**二つのIPブローカーのマーケットプレイスから、リース可能なすべてのプレフィックスと月額価格**を毎日収集
- リース推論データセット
  - **実際にインターネット上でルーティングされ活動的にリースされていると推測されるプレフィックスを特定するため**、RouteViews、RIPE RIS などの**BGPデータ**、月次**WHOISデータ**、**AS関係データ**などを統合し、2024年9月から2025年2月までの月次スナップショットを収集
- FireHOL IP リスト(ブロックリスト)
  - 様々な形態の**ネットワーク不正利用を間接的に測定**するための指標とするため、 2024年1月1日から2025年3月12日まで、複数のブロックリストを網羅的に集約した**「FireHOL IPリスト」のデイリースナップショット**を収集
  - FireHOL： Linuxファイアウォール管理を簡素化するために設計されたオープンソースのフレームワーク
  - https://iplists.firehol.org/
- BGPルーティング情報ベース(RIB)データ
  - リースされたプレフィックスの不正利用率を比較するため、**リースされていないアドレス空間**の中から、**ルーティングされているプレフィックスをランダムにサンプリング**
- データの一部は以下のURLで公開
  - https://doi.org/10.5281/zenodo.15398237

論文紹介『IPv4リース市場における不正利用の調査』-4-

- リースされているプレフィックスの特定方法(推論)は？
- 前述のデータを元に、**WHOIS情報に登録されているIPホルダーと、実際にそのプレフィックスをアナウンスしている組織との間に、既知のインターネット上での関連性（AS関係）がない場合に、そのプレフィックスがリースされている**と判断
- この特定方法は課題が存在するが、精度はかなり高い
  - ハイジャック、DDoS攻撃緩和サービス、マルチプルオリジン
  - 「リースされている」と推定されたプレフィックスのうち、実際にリースであったプレフィックスの割合：**98%**
  - 実際にリースされていたプレフィックスの総数のうち、正しくリースとして検出できたプレフィックスの割合：**82%**

論文紹介『IPv4リース市場における不正利用の調査』-5-

- 分類種別は？
- FireHOLが集約している253のブロックリストとそのカテゴリを利用
  - **abuse**：自動化されたウェブスクリプト(ボット)
  - **anonymizers**：オープンプロキシやTorノード のような匿名化サービス
    - 著者は、『このサービス自体は本質的に不正を示すものではないものの不正利用を可能にする可能性があるため分析に含める』ことを選択
  - **attacks**：さまざまな形態のハッキングやオンラインの脅威
  - **malware**：ワーム、コマンド＆コントロール（C2）サーバー、およびマルウェアを配布
  - **reputation**：犯罪行為 や 有害なコンテンツの共有
  - **spam**：電子メール SPAM
  - これらは除外：**organizations、unroutable**

論文紹介『IPv4リース市場における不正利用の調査』-6-

- 対象期間: 2025/1/11～2/10
- 方法：推定されたリースプレフィックス(62,944個)と、それと同数で同じサイズのランダムにサンプリングされた非リースプレフィックスを前述のブロックリストで調査
  - リースされているプレフィックスは全ルーティングプレフィックスの**6.10%**
- 結果：**リースされているプレフィックスは非リースプレフィックスと比較して、ブロックリストにフラグが立てられる可能性が2.89倍高い**
- **Anonymizers**で最も差が大きく**2.59倍**、SPAMはリースプレフィックスの方が非リースプレフィックスより**1.55倍低い**

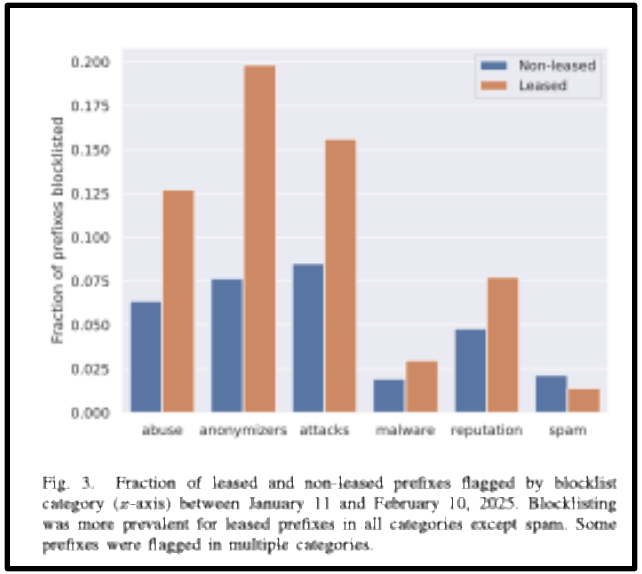


Fig. 3. Fraction of leased and non-leased prefixes flagged by blocklist category (*x*-axis) between January 11 and February 10, 2025. Blocklisting was more prevalent for leased prefixes in all categories except spam. Some prefixes were flagged in multiple categories.

論文紹介『IPv4リース市場における不正利用の調査』-7-

- リース開始後のブロックリスト登録数の推移は？
  - プレフィックスのリース開始後から登録数は増加し続け、**測定期間の最後まで上昇傾向**
  - **不正利用のほとんどは比較的速く検出**され、全カテゴリの中央値検出時間は27日
  - **リース開始から150日後(約5ヶ月後)**の時点で、ブロックリストへの登録率がカテゴリによって**大きく増加**
    - **abuse、anonymizers、attacksは顕著な増加**

- anonymizers(オープンプロキシやTorノード)を利用しabuseやattacksが行われている
- 悪意のあるアクターはリースされたIPアドレスを頻繁に**ローテーションしていない**可能性が高い

論文紹介『IPv4リース市場における不正利用の調査』-8-

- 価格との相関関係
  - プレフィックスの1ヶ月あたりの**リース価格と過去のブロックリスト登録件数**との間に**統計的に有意な相関関係は見つからなかった**
  - つまり…
    - リース会社が過去の不正利用を開示しない、
    - リース会社がリース期間中に発生した不正利用に気づいていない
  - (私見)：意図的に秘密にしている、もしくは外部からの指摘を無視している？！？！？！？！
- その他の興味深い指摘
  - アドレスリースにおけるRPKIは借用者(悪意のあるアクター)に対して一時的ではあるが**正当な使用権限を与えてしまう**のではないか？

論文紹介『IPv4リース市場における不正利用の調査』-9-

- 関連研究
  - Sublet Your Subnet: Inferring IP Leasing in the Wild
    - https://dl.acm.org/doi/10.1145/3646547.3689010
    - Abstractより意訳
      - 2024/4時点で広報されている全IPv4プレフィックスの4.1%がリースプレフィックス
      - リースされたアドレス空間は、非リース空間と比較して約5倍不正利用される可能性が高い
  - A First Look at the Misuse and Abuse of the IPv4 Transfer Market
    - https://link.springer.com/chapter/10.1007/978-3-030-44081-7_6
    - Abstractより意訳
      - 2009年10月から2019年8月の期間において、移転されたプレフィックスは、非移転プレフィックスと比較して、ブロックリストに4倍から43倍も多く登録される傾向にあることが判明
      - 悪意のあるネットワークが評判によるペナルティを回避するために「クリーンな」アドレス空間を取得するか、ブロックリストに載ったアドレスを処分する機会として移転を利用している可能性がある

論文紹介『IPv4リース市場における不正利用の調査』-10-

- この論文を調べていて、気がついたこと
- **Cogent**は同社が保有する**IPv4アドレスを担保として債券を発行**し、2億600万米ドルの資金をゲット
  - https://www.cogentco.com/en/about-cogent/press-releases/4443-cogent-announces-ipv4-address-securitization-offering
- IPv4.Globalが**IPアドレスを担保とした融資**プログラムを開始
  - https://www.ipv4.global/press-releases/ipv4-lending/

- (私見)IPv4アドレスは**企業の財務活動を裏付ける正式な流動性の高い資産**へと変化？？
- (私見)IPv4アドレスの売買やリースなどの市場が、単なる技術的な取引を超え、**高度に金融化された市場**へと進化しつつある？？