国内悪性プロキシサービスとの闘争

2022/01/27

株式会社リクルート

猪野　裕司

自己紹介

- 猪野裕司
  - 株式会社リクルート
  - セキュリティ統括室
  - サイバー犯罪対策グループ
- 2016年株式会社リクルート テクノロジーズ入社、リクルートCSIRTとして、リクルートで発生するセキュリティ事故への対応をリード。
- CISSP、GCIH、GCTI、GNFA

注意

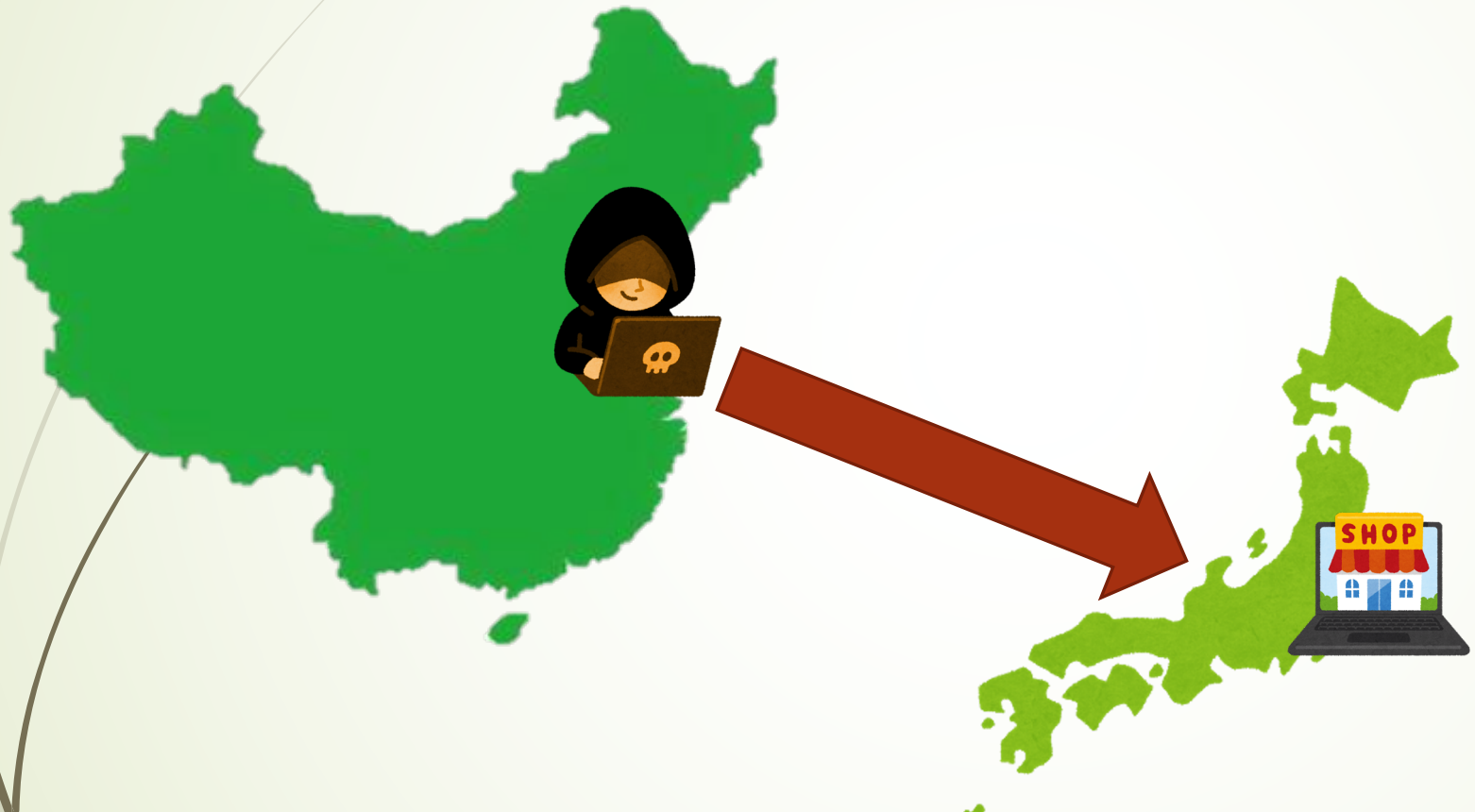
- この資料は、国内に存在する悪性プロクシの現状を共有することを目的としています。
- この発表は発表者の所属を代表するものではありません。また、講演中に紹介する個別事例についても、所属とは関係はありません。

アジェンダ

- レジデンシャルプロクシとは
- はじめに
- サイバー犯罪の現状

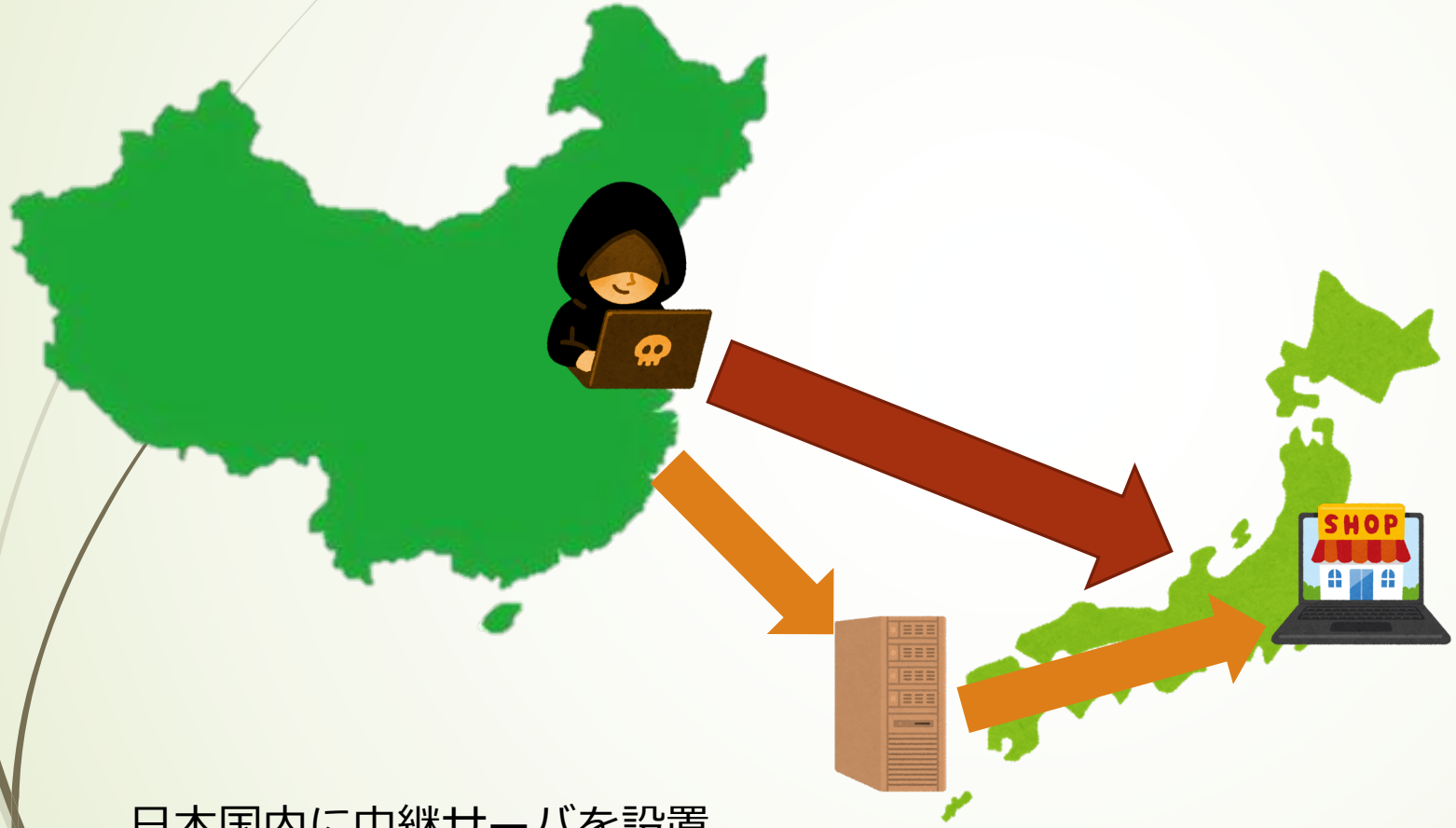
- データの分析と活用
- まとめ

悪性レジデンシャルプロクシとは



日本国内向けのサービスに対し、海外からのアクセスすると不正がバレる

悪性レジデンシャルプロクシとは



日本国内に中継サーバを設置。
アクセス元を国内にすることで不正検知を回避

悪性レジデンシャルプロクシとは

不正アクセスの疑い、中継サーバー業者を捜索
警視庁など

2014年11月19日 11:57

保存

不正に入手した他人のIDやパスワードを使ってインターネット接続業者にアクセスしたとして、警視庁は19日、不正アクセス禁止法違反の疑いで、東京都内のサーバー管理業者などを家宅捜索した。容疑が固まり次第、関係者らを逮捕する方針。京都、埼玉など10以上の府県警も同日、各地で管理業者の一斉摘発に乗り出した。

業者はネット接続を中継する「プロキシサーバー」を管理している。プロキシサーバーを経由するのは本来、接続速度を速くするなどの目的があるが、ネット上の番地に当たる「IPアドレス」が置き換わり、発信元の特定が難しくなるため、サイバー犯罪の温床になっていると指摘されていた。

捜査関係者によると、都内の管理業者のプロキシサーバーを経由して、何者かが他人のIDやパスワードで接続業者にアクセスした形跡があった。管理業者は顧客が自社のサーバーを不正アクセスに使うのを認識していた疑いが持たれている。

プロキシサーバーを巡っては、警視庁などが2～4月、管理業者「中都商事」（東京・豊島）社長の中国籍の男らを不正アクセス禁止法違反や著作権法違反の疑いで逮捕。3月には同庁が、大手接続業者にプロキシサーバー業者と契約しないよう要請していた。〔共同〕

無届けで中継サーバー　ネット犯罪に使用か　千葉県警、中国人を逮捕　電気通信事業法違反容疑

2017年5月19日 10:36 | 無料公開

中国人らが海外のインターネットサイトを閲覧できるよう、中継サーバーを無届けで埼玉県内のシェアハウスに設置したとして、千葉県警サイバー犯罪対策課と千葉北署などは１８日、電気通信事業法違反の疑いで、中国籍の男で私立大学院生、李碩容疑者（２６）＝埼玉県吉川市＝を逮捕した。不正に設置した中継サーバーは犯罪の温床とされており、県警では新潟、山梨、和歌山、福岡、熊本各県警と合同捜査本部を設置し捜査していた。捜査本部では中国に首謀者がいるとみて調べている。

千葉県警などが押収したパソコンやルーターなど＝１８日午後、千葉北署

逮捕容疑は氏名不詳者と共謀し昨年３月２６日～１０月３１日、埼玉県戸田市内の一戸建て住宅に、インターネットの中継サーバーを設置し、国外などの不特定多数の利用者からの通信を多数回にわたり無届けで中継するなどした疑い。李容疑者は「届け出をしないでサーバーコンピューターを設置、管理していた」と容疑を認めている。

同課によると、中国国内の一般ネット利用者は海外サイトに接続できないため、日本国内に中継サーバーを設置。中国の首謀者が一般から料金を得ていたとみられる。李容疑者はこの中継サーバーを設置して保守管理や接続料金の支払いなどを担当。首謀者から中国の電子マネーで月数万円程度の報酬を受け取っていたとみられる。

中継サーバーは、シェアハウスとなっている一戸建て住宅の１室に設置され、パソコン５台にルーター３２台を接続。パソコン内には仮想サーバー１８０台が確認された。海外からの利用者は主に中国人で、ＩＰアドレスで約１６００人分。利用者のＩＰアドレスは中継サーバーを介して日本のＩＰアドレスに変換される仕組みで、利用者は日本国内のさまざまなサイトに接続できるようになっていた。

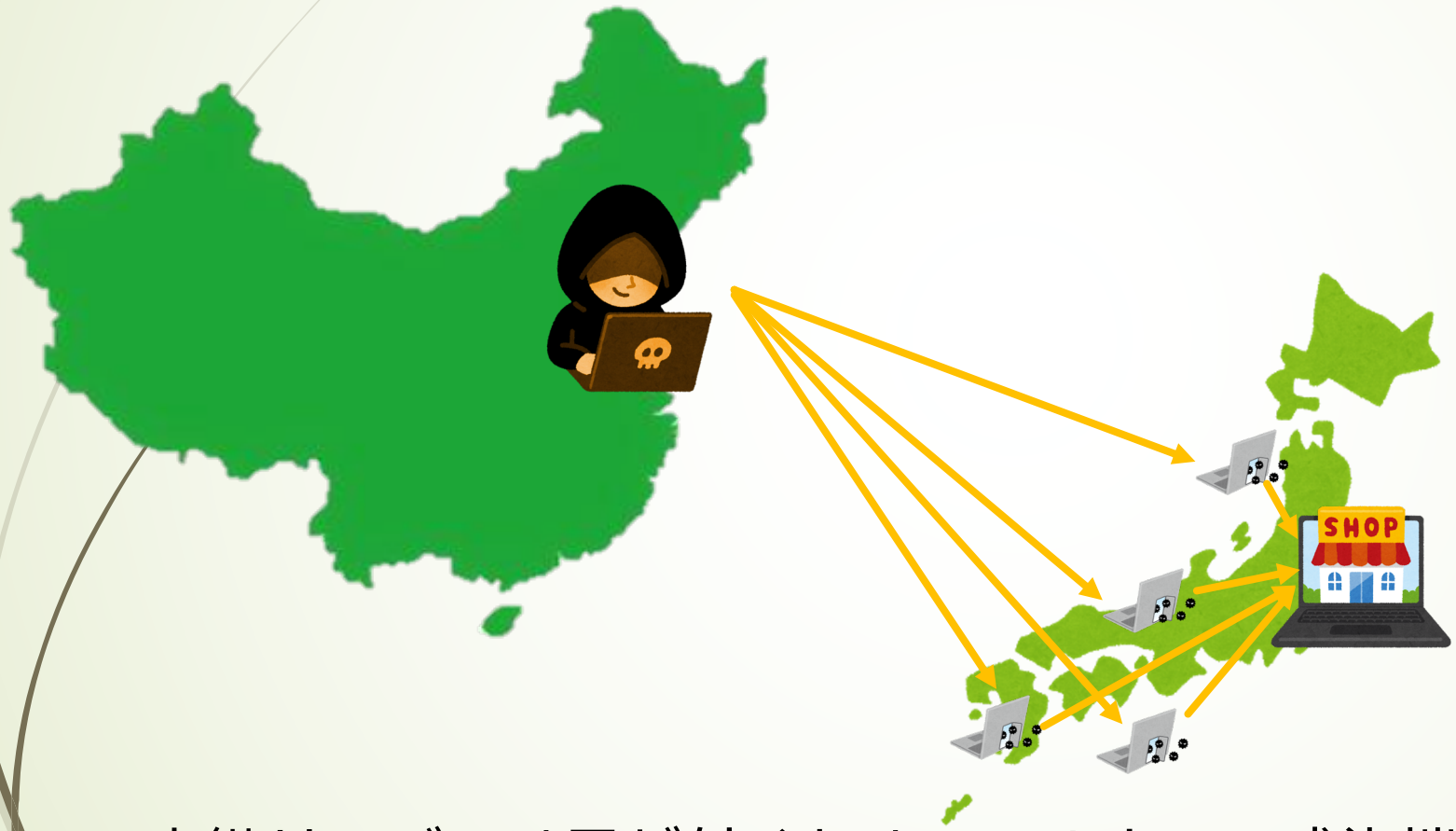
県警で昨年６月以降、県内の銀行でネットバンキングに対する不正送金事案を調べていたところ、この中継サーバーを特定。県外でもネット関連の犯罪で使用されていたことが判明した。

李容疑者はシェアハウス１室のカギを所持して中継サーバーを管理。この部屋の契約には別のアルバイトが関与していたという。

日本国内に中継サーバを設置
アクセ

2014年　各地で一斉摘発
2017年　中国留学生逮捕　→　中継サーバインフラは摘発

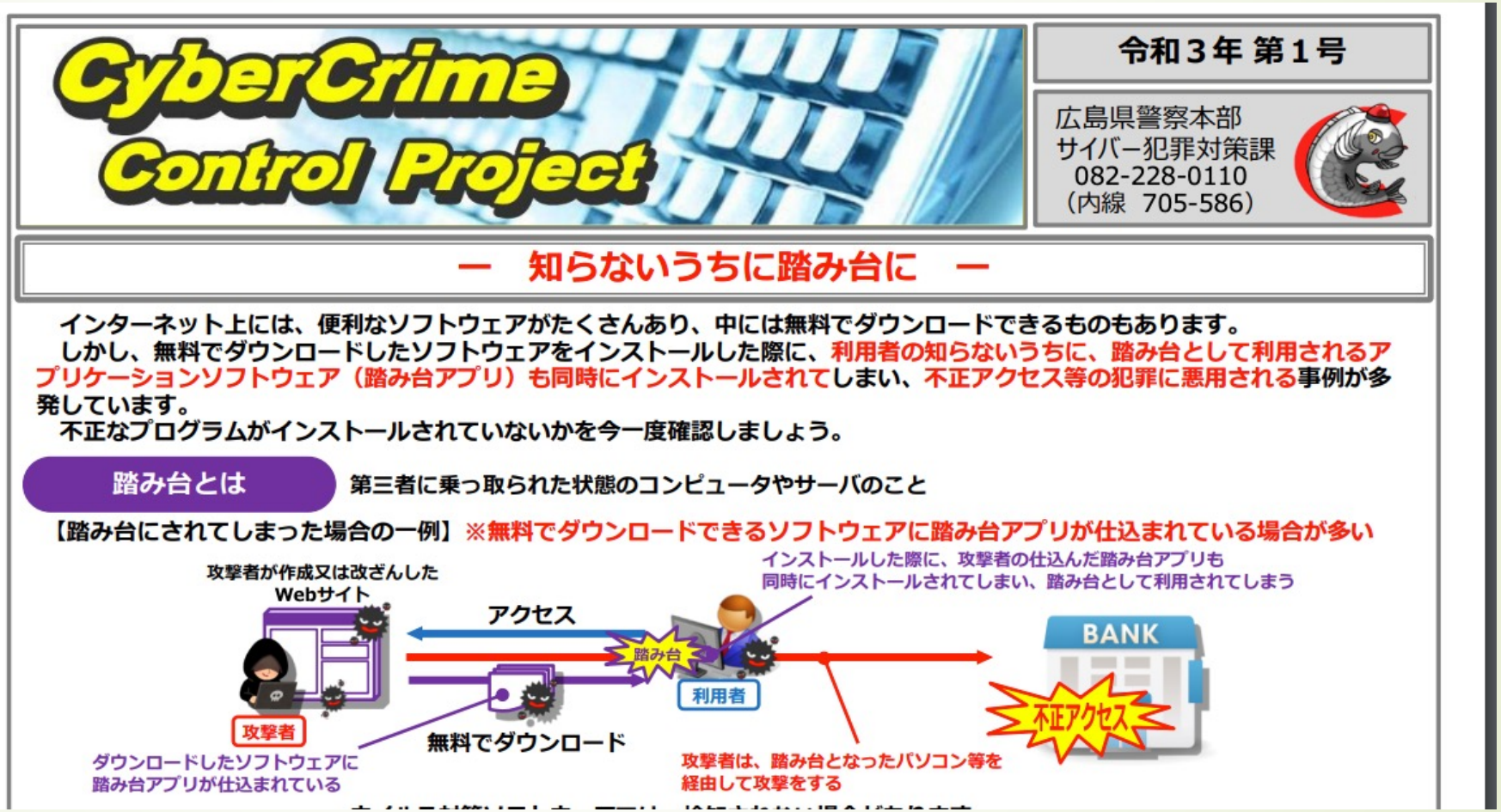
悪性レジデンシャルプロクシとは



中継サーバでは足が付くため、マルウェア感染端末を利用した
RESIP(Residential IP)プロクシに犯罪インフラが移行

悪性レジデンシャルプロクシとは

- 広島県警が注意喚起



https://www.pref.hiroshima.lg.jp/uploaded/attachment/417114.pdf

悪性レジデンシャルプロクシとは

- 資料の中で2つのプログラムに言及。

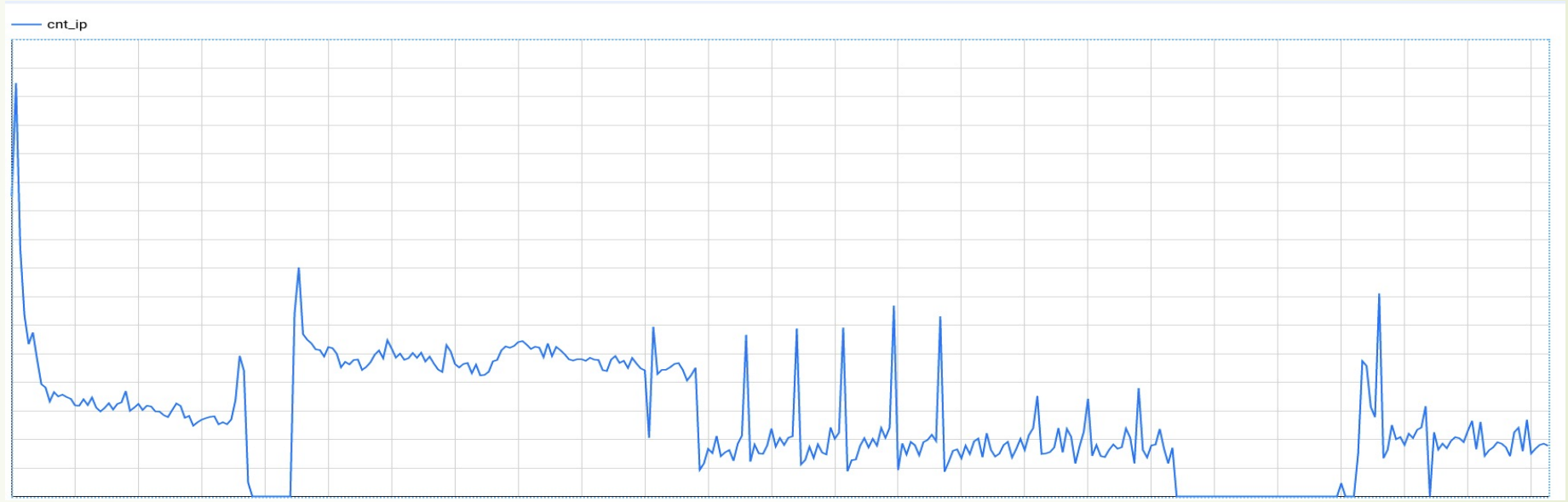
https://www.pref.hiroshima.lg.jp/uploaded/attachment/417114.pdf

はじめに　（調査のきっかけ）

- カード不正利用している特定のアクターXを追いかけていた。
- 調査の結果、Xの生IPアドレスは判明した。
- ログを分析したところ、カード不正利用時のアクセスはXではない第三者のアクセス、しかも、国内IPアドレスだった。
- このIP契約者はアクターXとは関係ない第三者だった。パソコンがマルウェアに感染。
- 「このマルウェアプロクシのIPを収集して、不正対策に活用できないか・・？」

何をやったのか

- RESIPプロクシのIPアドレスを収集して分析



収集したデータ

- IPの統計データ

IPアドレス　発見日　最終観測日　位置　ASN　出現頻度　出現日　出現期間

行	ip_address	first_seen	last_seen	city	asn	occurrences	days	date_diff
1	14.10.[redacted]	2021-01-18 07:46:34 UTC	2022-01-17 02:58:24 UTC	Suita	KDDI	708	256	364
2	14.14.[redacted]	2021-01-18 13:57:17 UTC	2022-01-16 01:43:08 UTC	Yonago	KDDI	722	255	363
3	111.98.[redacted]	2021-01-18 19:58:59 UTC	2022-01-16 03:57:59 UTC	Setagaya-ku	au one net	730	251	362

- 詳細データ

出現時刻（UNIXTIME）　IPアドレス　位置　ASN　記録日

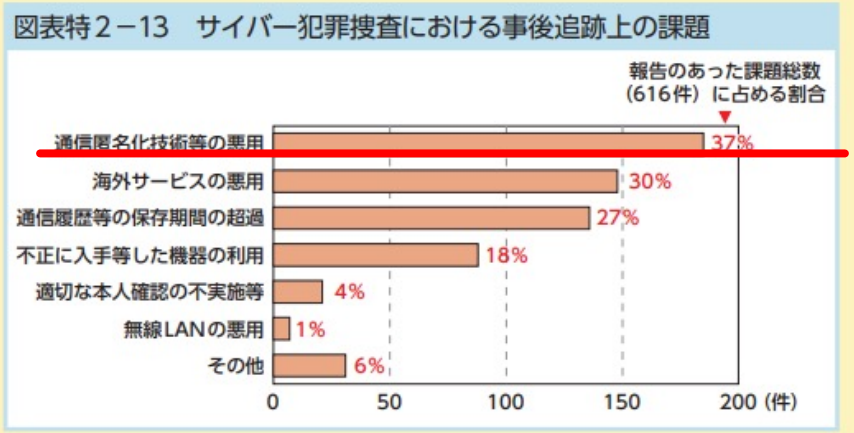
行	unixtime	ip_address	city	asn	date
1	1642384247	153.232[redacted]	Ibaraki machi	DTI	2022-01-17
2	1642394616	153.232[redacted]	Ibaraki machi	DTI	2022-01-17
3	1642384334	114.149[redacted]	Hachinohe	DTI	2022-01-17
4	1642391831	114.149[redacted]	Hachinohe	DTI	2022-01-17

収集当初は統計データのみだったが、過去分析目的として詳細データを作成

サイバー犯罪の現状

MEMO サイバー犯罪捜査における犯人の事後追跡上の課題

サイバー犯罪捜査における犯人の事後追跡可能性について、都道府県警察本部のサイバー犯罪対策担当課に対し、令和元年中に認知したサイバー犯罪事件に関し、犯人の事後追跡上の課題となったものを調査したところ(注3)、プロキシ等の「通信匿名化技術等の悪用」が最も多く、次いで、「海外サービスの悪用」、捜査の時点で通信履歴（ログ）が保存されていないなどの「通信履歴等の保存期間の超過」が多かった。



こうした課題に対処するため、警察では、関係事業者等に対し、総務省の「電気通信事業における個人情報保護に関するガイドライン」を踏まえた通信履歴の適切な保存、適切な本人確認・認証等の実施を要請している。

ところ(注3)、プロキシ等の「通信匿名化技術等の悪用」が最も多く、次い

令和3年　警察白書
https://www.npa.go.jp/hakusyo/r03/pdf/03_tokushu02.pdf

サイバー犯罪の現状

ここのアクセスにRESIPが利用

追跡！サイバー犯罪組織　コロナ禍の日本を狙う闇
https://www.nhk.or.jp/gendai/articles/4631/index.html

サイバー犯罪の現状

海外実行犯は国内に痕跡を残さず犯罪を実施

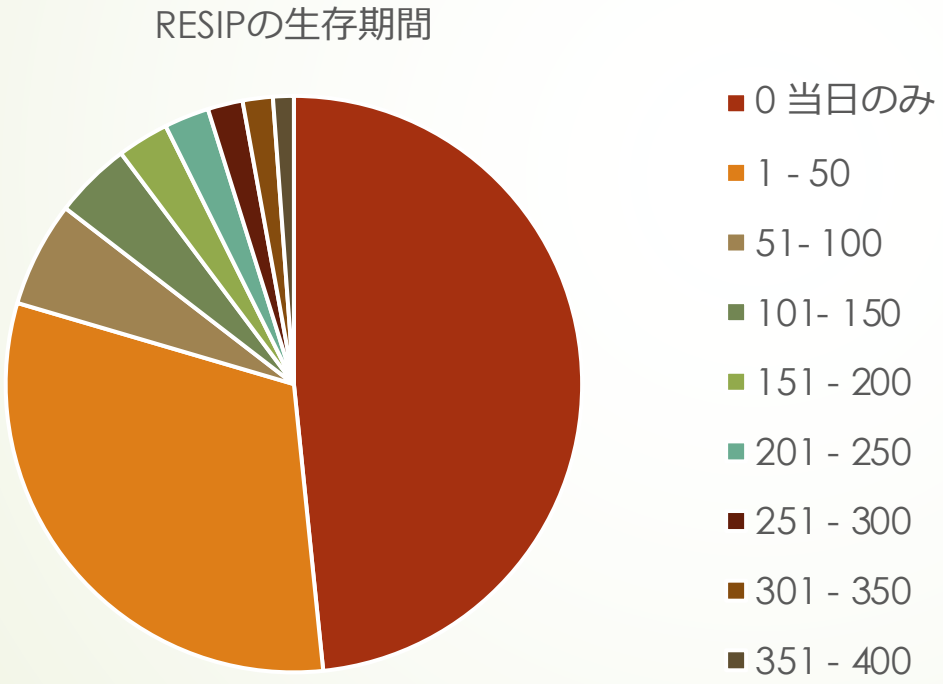
悪性RESIP利用＝犯人捜査が困難

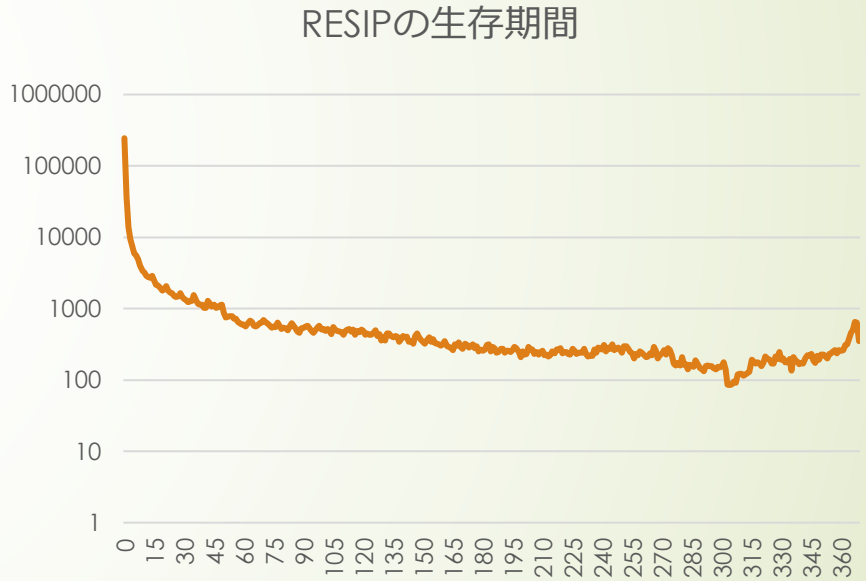
RESIPデータの分析

- 結論：目立った特徴がないのがRESIPの特徴。

RESIPデータの分析

- IPごとの生存期間　(date_diff = last_seen – first_seen)
- 5割のIPが1日しか出現しない。



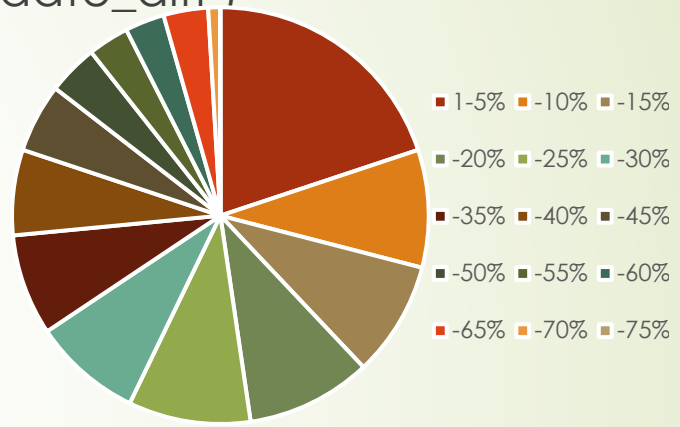


RESIPデータの分析

- 長期活動が観測されるIPにおけるアクティブ率 (days / date_diff)

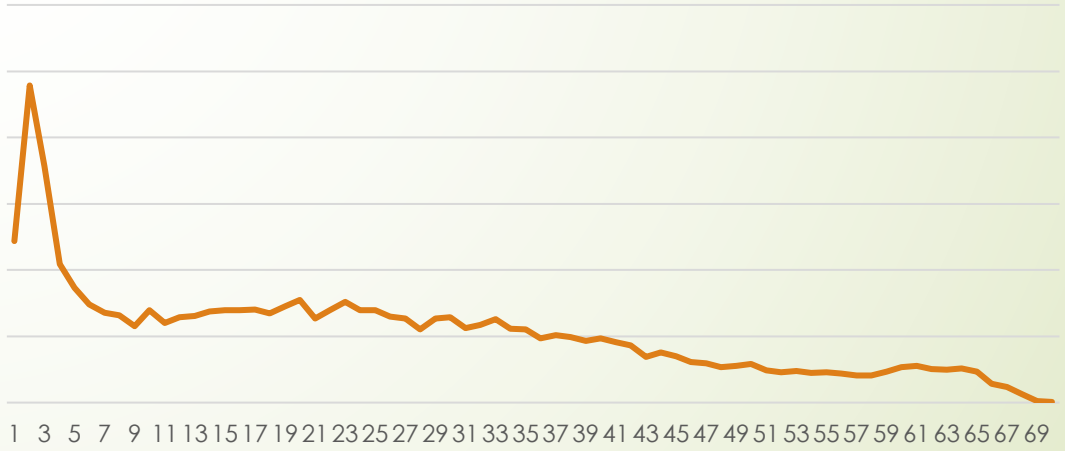
  days 出現が観測された日数

  生存期間が 300日以上に対して分析



約30% が観測日数が30日以下

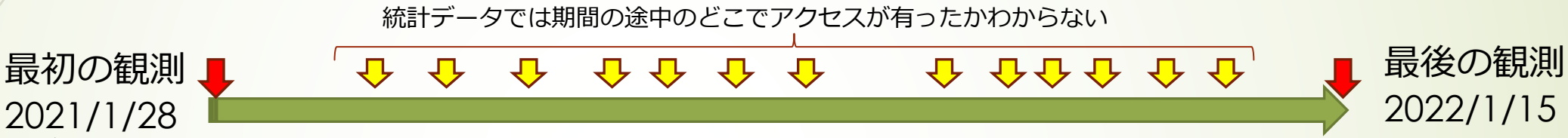
→ **長期間生存するIPであったとしても、常に悪性とは限らない**



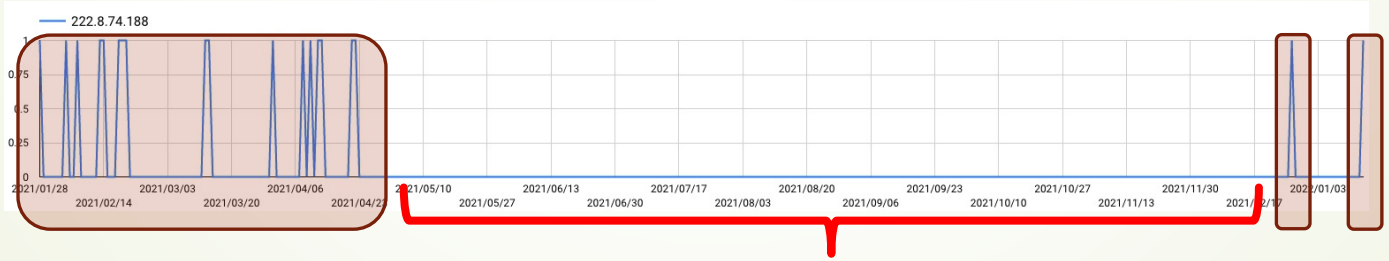
RESIPデータの分析

- 統計データの問題点

ip_address	days	first_seen	last_seen	date_diff
222.8.[redacted]	19	2021/1/28	2022/1/15	352



- 直近のログの突合には問題なかったが、過去データの分析において、不正発生時点でのプロクシ存在が判定できない。
- 取得時の生データを保存していたので、詳細データを生成



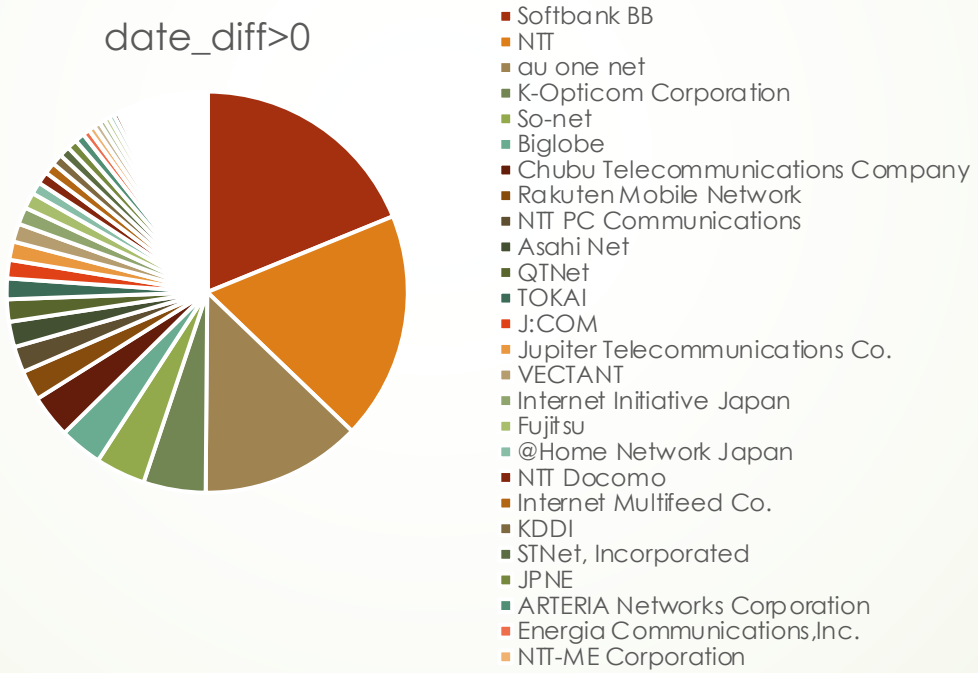
RESIPとの関連性強い

この間に事件があっても、
RESIPとの関連性が弱い

行	unixtime	ip_address	date
1	1611795448	222.8[redacted]	2021-01-28
2	1611795506	222.8	2021-01-28
3	1612429028	222.8	2021-02-04
4	1612652208	222.8	2021-02-07
5	1613188622	222.8	2021-02-13
6	1613285815	222.8	2021-02-14
7	1613620622	222.8	2021-02-18
8	1613689001	222.8	2021-02-19
25	1619013394	222.8	2021-04-21
26	1619062088	222.8	2021-04-22
27	1619087685	222.8	2021-04-22
28	1640564592	222.8	2021-12-27
29	1640566119	222.8	2021-12-27
30	1640568210	222.8	2021-12-27
31	1640568212	222.8	2021-12-27
32	1642212280	222.8	2022-01-15

RESIPデータの分析

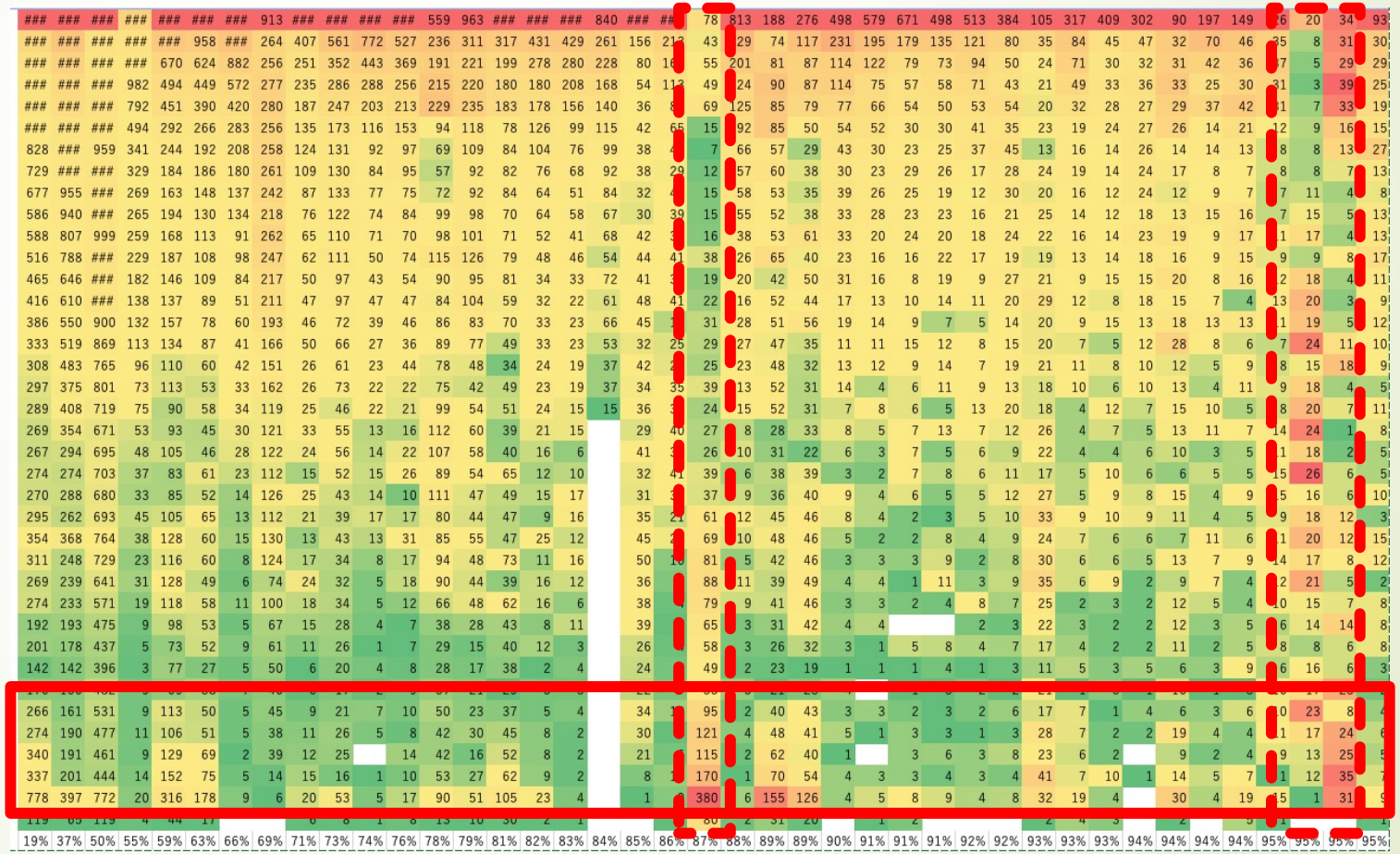
- date_diff>0のデータに対し、キャリアごとの集計。
- 特に突出したASNは見つからず。
- 特徴的な差異は見当たらなかった。



asn	割合	累積
Softbank BB	19%	19%
NTT	18%	37%
au one net	13%	50%
K-Opticom Corp	5%	55%
So-net	4%	59%
Biglobe	3%	63%
Chubu Telecomr	3%	66%
Rakuten Mobile	2%	68%
NTT PC Commu	2%	71%
Asahi Net	2%	73%
QTNet	2%	74%
TOKAI	2%	76%
J:COM	1%	78%
Jupiter Telecom	1%	79%
VECTANT	1%	81%
Internet Initiativ	1%	82%
Fujitsu	1%	83%
@Home Networl	1%	84%
NTT Docomo	1%	85%
Internet Multifee	1%	86%
KDDI	1%	87%
STNet, Incorpor	1%	88%
JPNE	1%	89%
ARTERIA Netwo	1%	89%
Energia Commu	1%	90%
NTT-ME Corpor	1%	90%

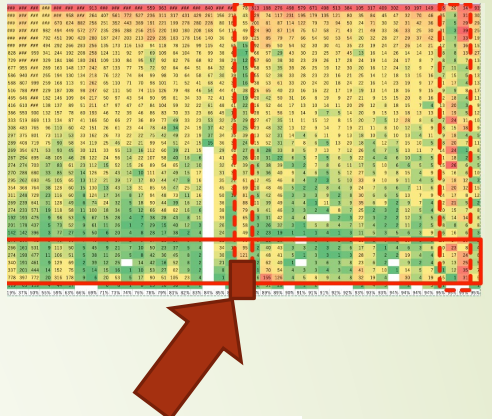
RESIPデータの分析

- キャリアごとの生存期間を集計。全体的に長期間生存IPが存在する。
- 長期生存IPが多いASNが3つある。 (赤点線枠)

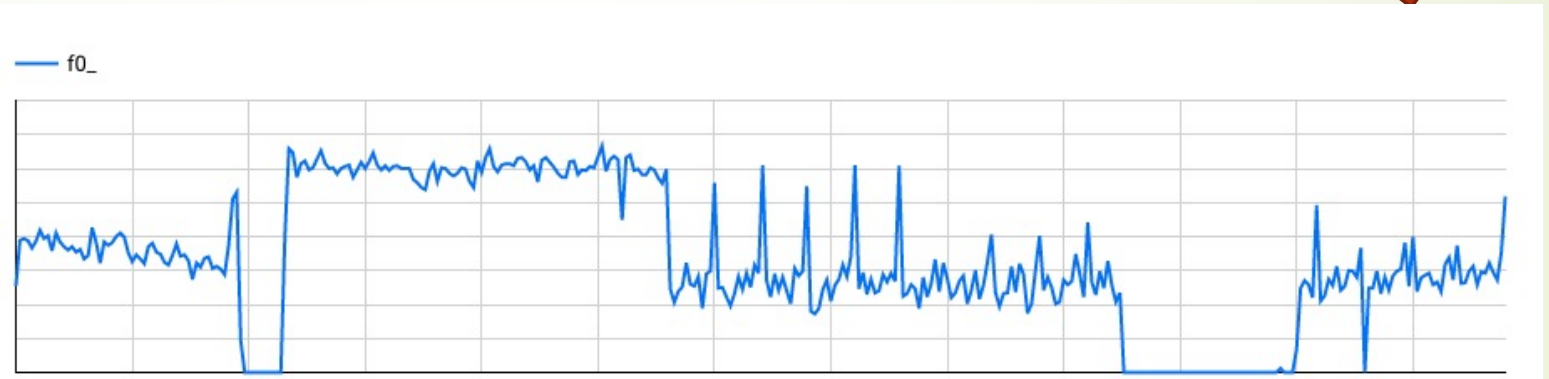


長期間生存するIPが存在

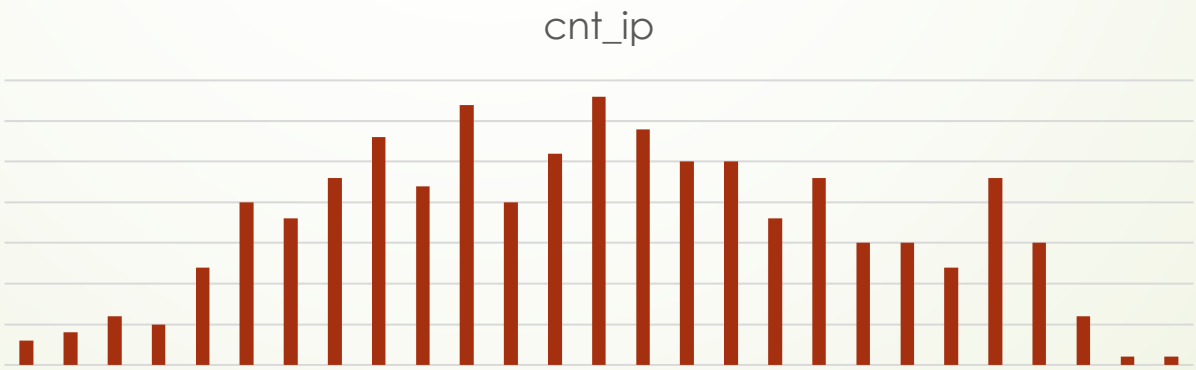
RESIPデータの分析



- 中央のASNを分析。360日以上生存しているIP460件。
- 日毎に出現したユニークなIP数（P14とほぼ同じ波形）



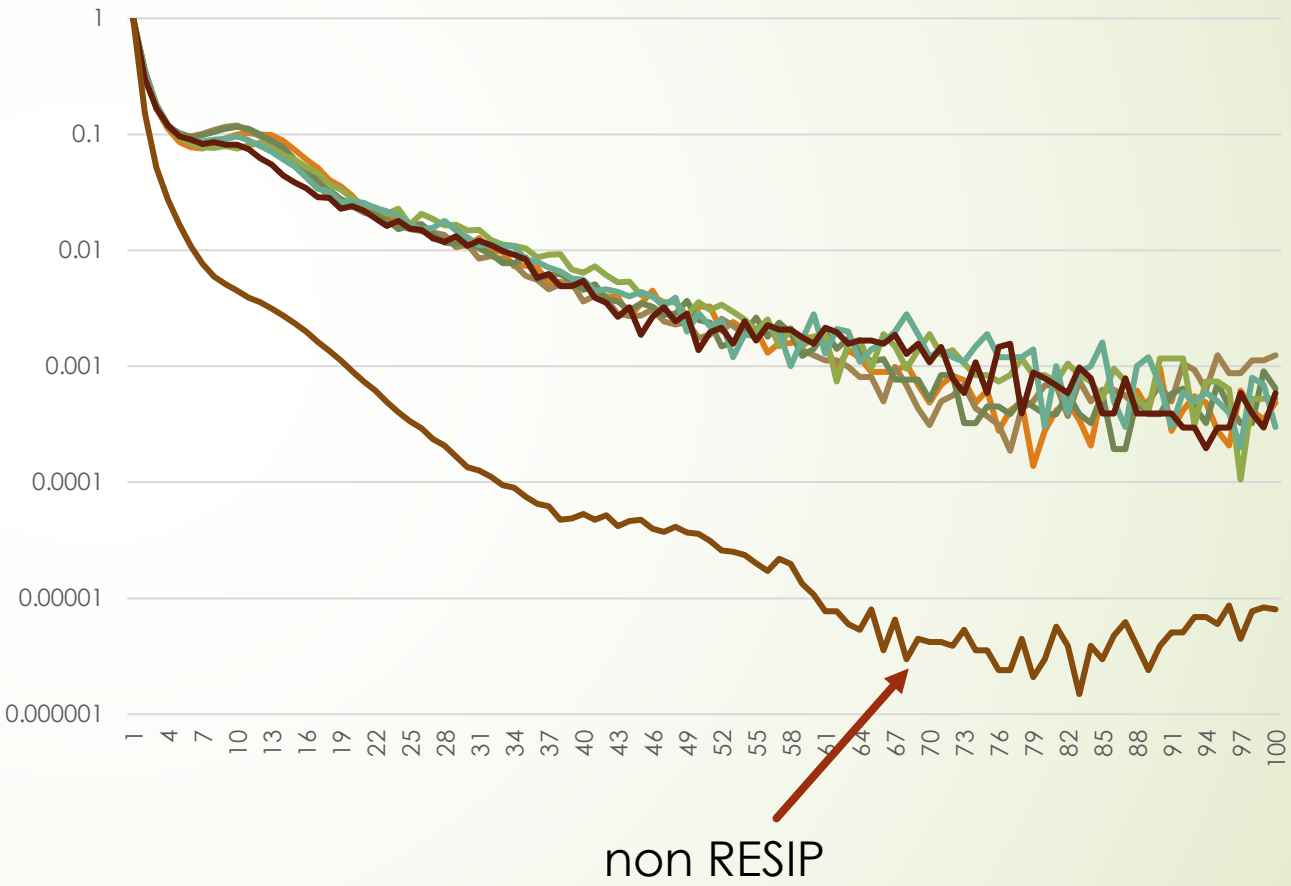
- 出現日数もごとのIP数も特に特徴なし



IPごとのユニークユーザーアクセス RESIP と non RESIP の比較

- RESIP と non RESIPの比較
- IPごとにユニークユーザーをカウントし、ユーザー数ごとにIP数を1ヶ月単位で集計。比較のため、一番高い数値で割り、対数グラフを作成
- 例：9IDに紐づくIPが1337件

  →1337/14397= 0.092
- RESIPの方が割合的に一つのIPからのアクセスID数が多い
- 10-15あたりが不自然に増加。
- これは1回の攻撃で利用されるアカウント数に関連していると推測。



RESIPデータの活用

- 収集したRESIPデータを用いて不正事案の検出ができないか検証。
- 事象としては「なりすましログイン」「盗難カードの不正利用」「詐欺」

- 突合の手法としては下記の2つの手法で実施。
  - すべてのトランザクションに対してRESIPデータを突合
  - 発生した不正データに対してRESIPデータを突合

全トランザクションに対して突合

- 事象は盗難カード不正利用
- 不正はチャージバックが発生トランザクションとする
- 単純なIPマッチで突合

検出不正件数/不正件数=　検出率97%　　不正件数/検出総数＝不正率3.2%

誤検知が多すぎるため役に立たない

- 詳細データを用いて事象発生時刻とRESIPの観測出現時刻の差分を算出、1Day以内を当たりとしたところ

検出不正件数/不正件数=　検出率22%　　不正件数/検出総数＝　不正率 47.1%

IP単体で判断すると結果は微妙。時刻との組み合わせが必須

検知漏れと誤検知のパターンの推測

- 検知漏れのパターン
  - 日時のクローリングで該当IPが収集できていなかった。

    元々のRESIPのデータ量が不明である。

    フィルタ「JP」として定期的にサーバからデータを取得。
    ランダムで戻ってきたIPをDBに格納。
  - 犯人がRESIPを利用していない。別のRESIPやVPNを使っている。

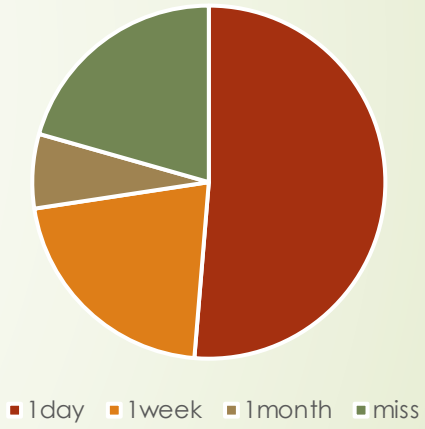
- 誤検知のパターン
  - 複数人が同一のIPでインターネット出口を共有（マンション型ネット回線、フリーWifiなど）
  - 携帯NW、モバイルWifi（頻繁にIPが変更）

    ー出口が頻繁にIPが変わる環境の場合、そもそも繋がるのか不明

不正データに対する突合

- なりすましログイン　事象A　同一アクター
  - 11件中10件1Dayヒット→ RESIP利用の可能性大
- 盗難カード不正利用　事象B　同一アクター
  - 21トランザクションがすべて1Dayヒット、100%マッチ→ RESIP利用の可能性大
- 投資詐欺　事象C　複数アクター
  - 1163ユニークIDによるアクセス元IP 573IP を分析。
    1Day hit率が半分を超える。

    → RESIP利用のアクターが存在
- カード不正　事象D
  - 34IPのうちIPヒット3件、しかも30日以上時間差あり
    → RESIP利用の可能性小　**すなわち、国内犯の可能性あり！**



同一アクターのアトリビューション判定には役に立つ。

まとめ

・RESIPのアドレスは常時更新され、短期間のIPが全体の半数以上。**不正なIPを収集しても、単純なIPアドレスブラックリストにならない**。

・誤検知を回避するためには、**IP出現時間も考慮した判定が必須**。データ単体で活用せず、トランザクションなど他の振る舞い情報もあわせた方がよい。

・アクターが**RESIP利用かどうかを判定するには有用**。（海外属性である可能性も判定可能）

おわり

一緒にRESIPを分析しませんか？

yumano@r.recruit.co.jp
twitter : @yumano