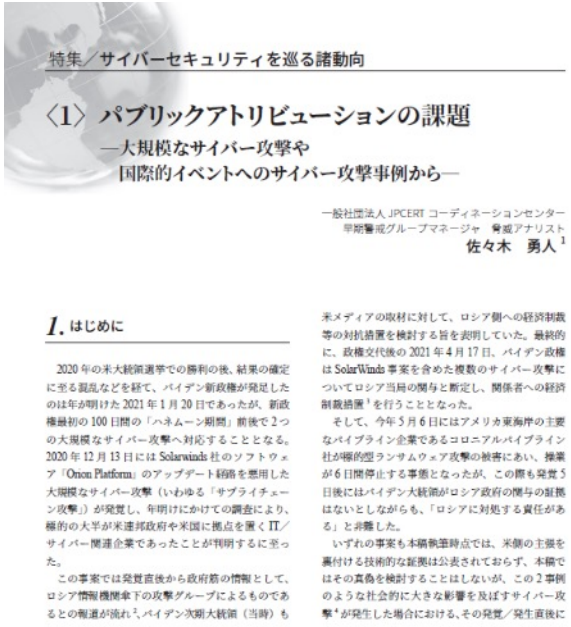
リアルタイムインシデント対応におけるアトリビューションの課題＋α

2021年9月13日
JPCERTコーディネーションセンター
早期警戒グループ マネージャ
脅威アナリスト
佐々木 勇人

今回書かせていただいたテーマ



特集／サイバーセキュリティを巡る諸動向

〈1〉パブリックアトリビューションの課題
—大規模なサイバー攻撃や
国際的イベントへのサイバー攻撃事例から—

一般社団法人 JPCERT コーディネーションセンター
早期警戒グループマネージャ　脅威アナリスト
佐々木　勇人[1]

1. はじめに

2020年の米大統領選挙での勝利の後、結果の確定に至る混乱などを経て、バイデン新政権が発足したのは年が明けた2021年1月20日であったが、新政権最初の100日間の「ハネムーン期間」前後で2つの大規模なサイバー攻撃へ対応することとなる。2020年12月13日にはSolarwinds社のソフトウェア「Orion Platform」のアップデート経路を悪用した大規模なサイバー攻撃（いわゆる「サプライチェーン攻撃」）が発覚し、年明けにかけての調査により、極的の大半が米連邦政府や米国に拠点を置くIT／サイバー関連企業であったことが判明するに至った。

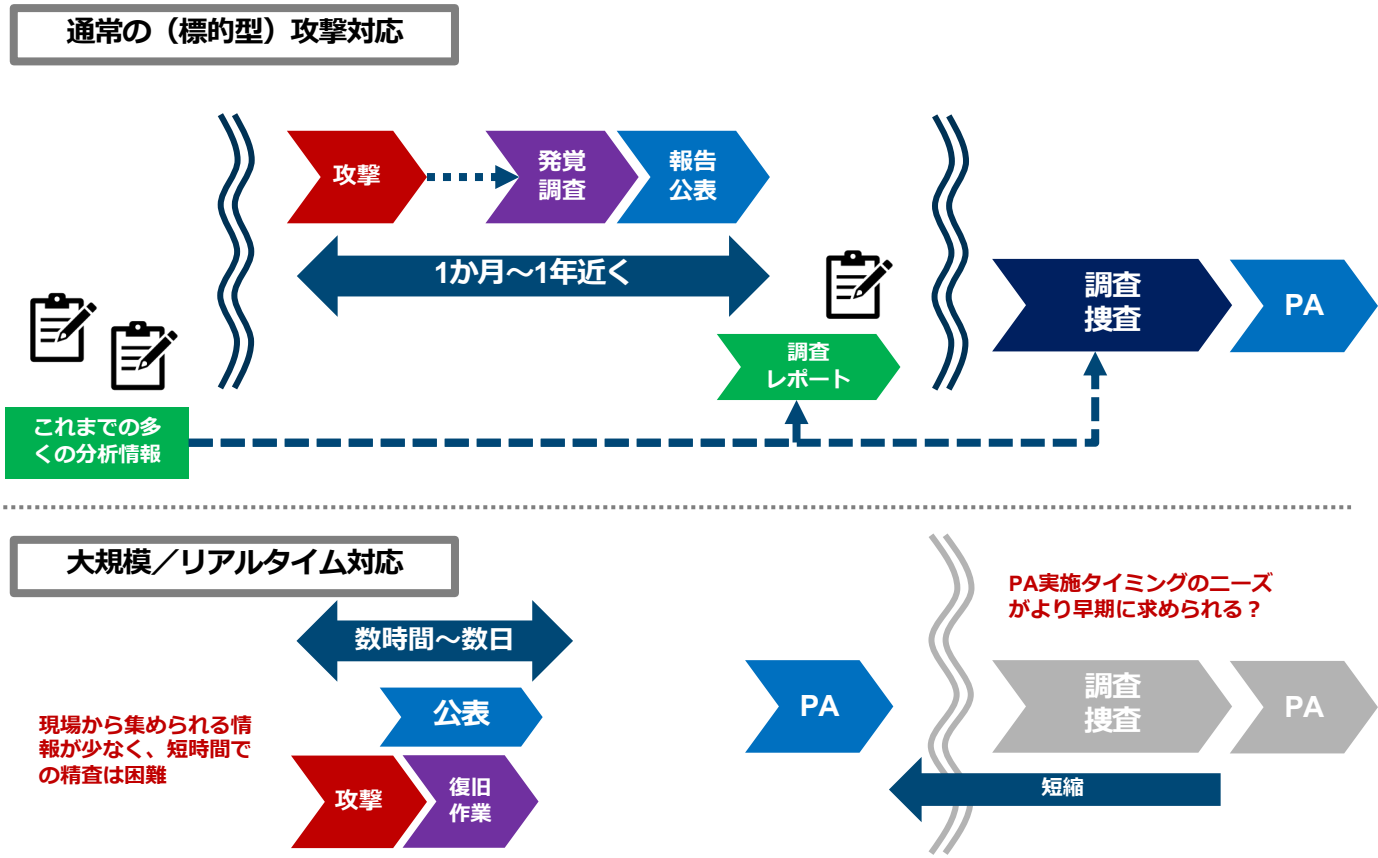
この事案では発覚直後から政府筋の情報として、ロシア情報機関傘下の攻撃グループによるものであるとの報道が流れ[2]、バイデン次期大統領（当時）も米メディアの取材に対して、ロシア側への経済制裁等の対抗措置を検討する旨を表明していた。最終的に、政権交代後の2021年4月17日、バイデン政権はSolarWinds事案を含めた複数のサイバー攻撃についてロシア当局の関与と断定し、関係者への経済制裁措置[3]を行うこととなった。

そして、今年5月6日にはアメリカ東海岸の主要なパイプライン企業であるコロニアルパイプライン社が極的型ランサムウェア攻撃の被害にあい、操業が6日間停止する事態となったが、この際も発覚5日後にはバイデン大統領がロシア政府の関与の証拠はないとしながらも、「ロシアに対処する責任がある」と非難した。

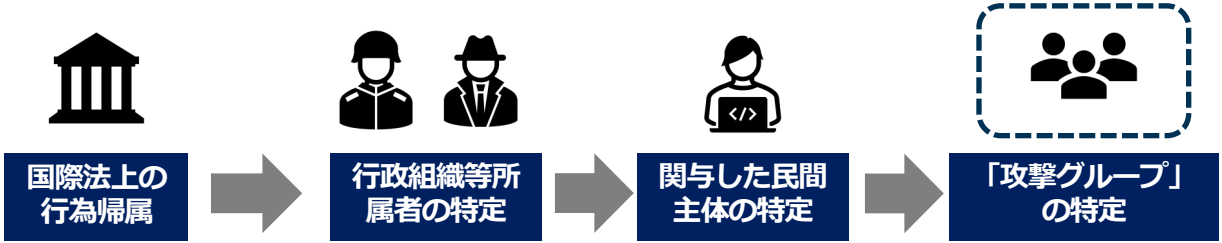
いずれの事案も本稿執筆時点では、米側の主張を裏付ける技術的な証拠は公表されておらず、本稿ではその真偽を検討することはしないが、この2事例のような社会的に大きな影響を及ぼすサイバー攻撃[4]が発生した場合における、その発覚／発生直後に

- CISTECジャーナル7月号に
  「パブリックアトリビューションの課題－大規模なサイバー攻撃や国際的イベントのサイバー攻撃事例から－」
  として掲載させていただきました
- ちなみに、9月号には
  「サイバー攻撃グループの“分類学”－国連安保理北朝鮮制裁委員会専門家パネルによる報告書から読み解く－」
  を寄稿予定です
  - －攻撃グループ「Lazarus」がどのような“サブグループ”で構成されているか考察
  - －11月のHITCON2021他、国際カンファレンスで同僚の発表（2020年に見つかった新たなマルウェア、手口の解析）の“オマケ”として発表予定

インシデント対応⇒PAまでの「時間軸」の比較



アトリビューションの「粒度」



技術レポート

※攻撃者のOpsecミスなど

OSINTによる実行者特定

技術レポート

※所在地域や組織的背景の推測

状況証拠による指摘

技術レポート

ソフト／広義のアトリビューション

刑事手続き＋α

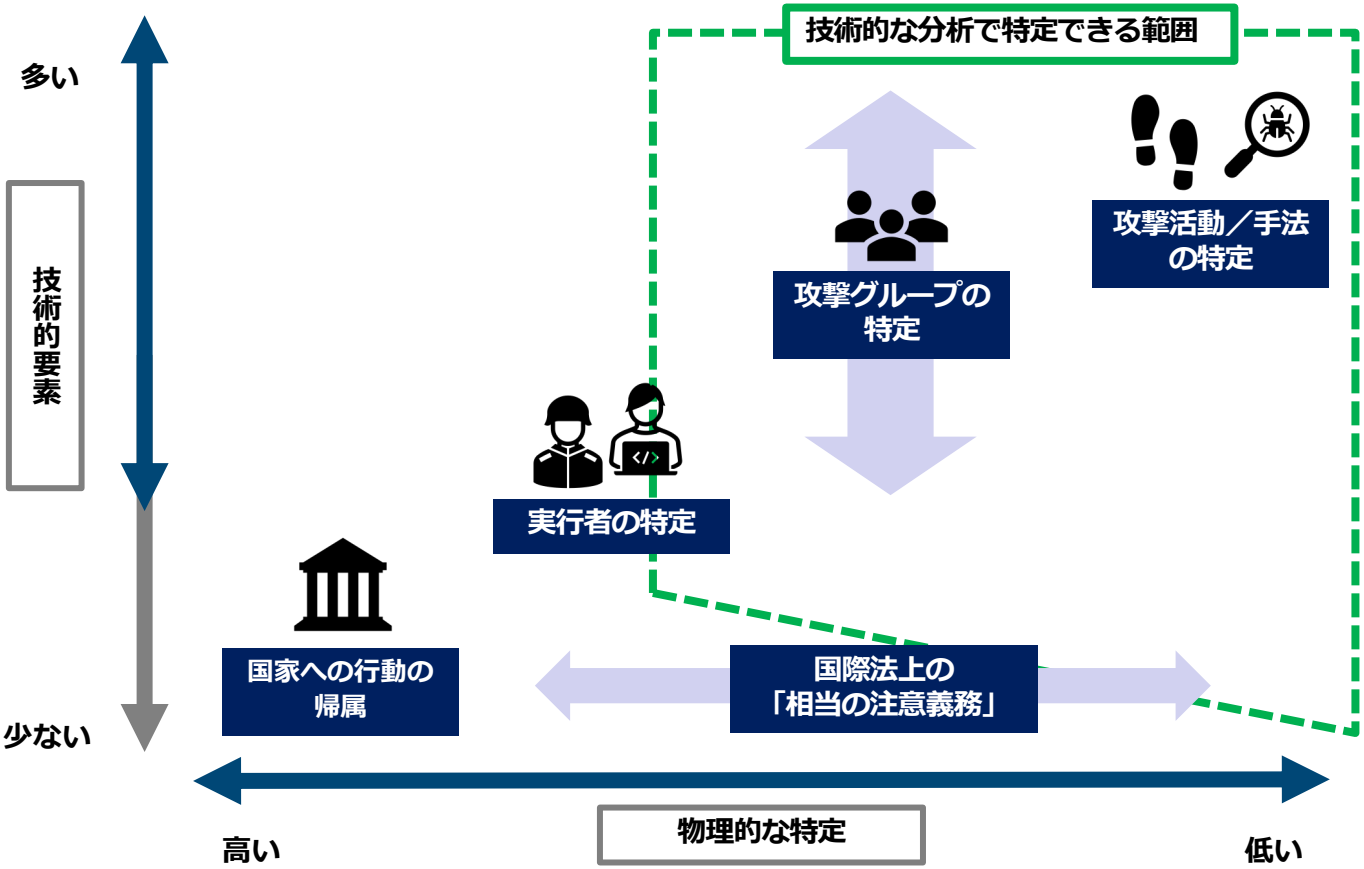
技術レポート

相当の注意義務 指摘？

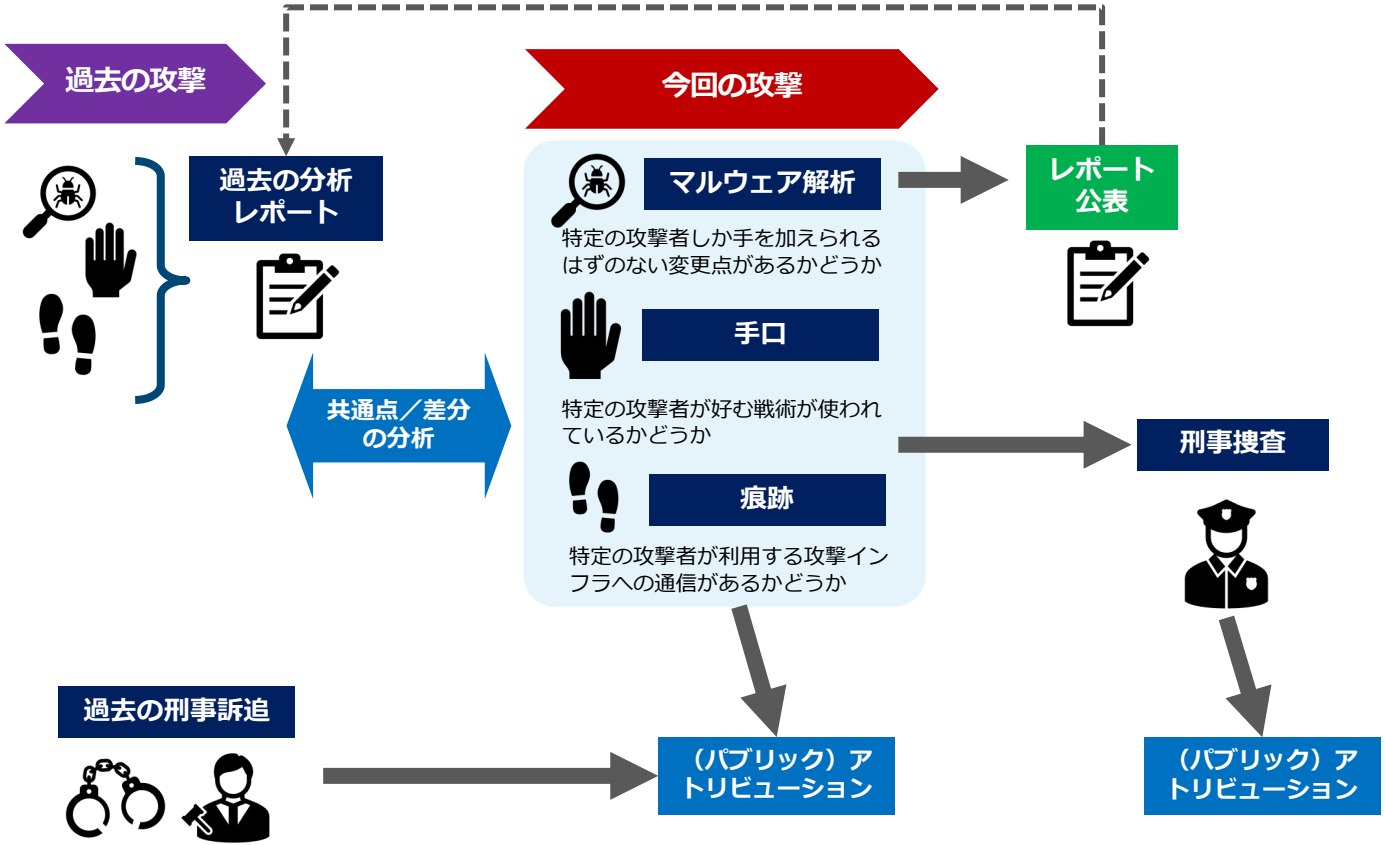
技術レポート

ハード／狭義のアトリビューション

アトリビューションの「粒度」

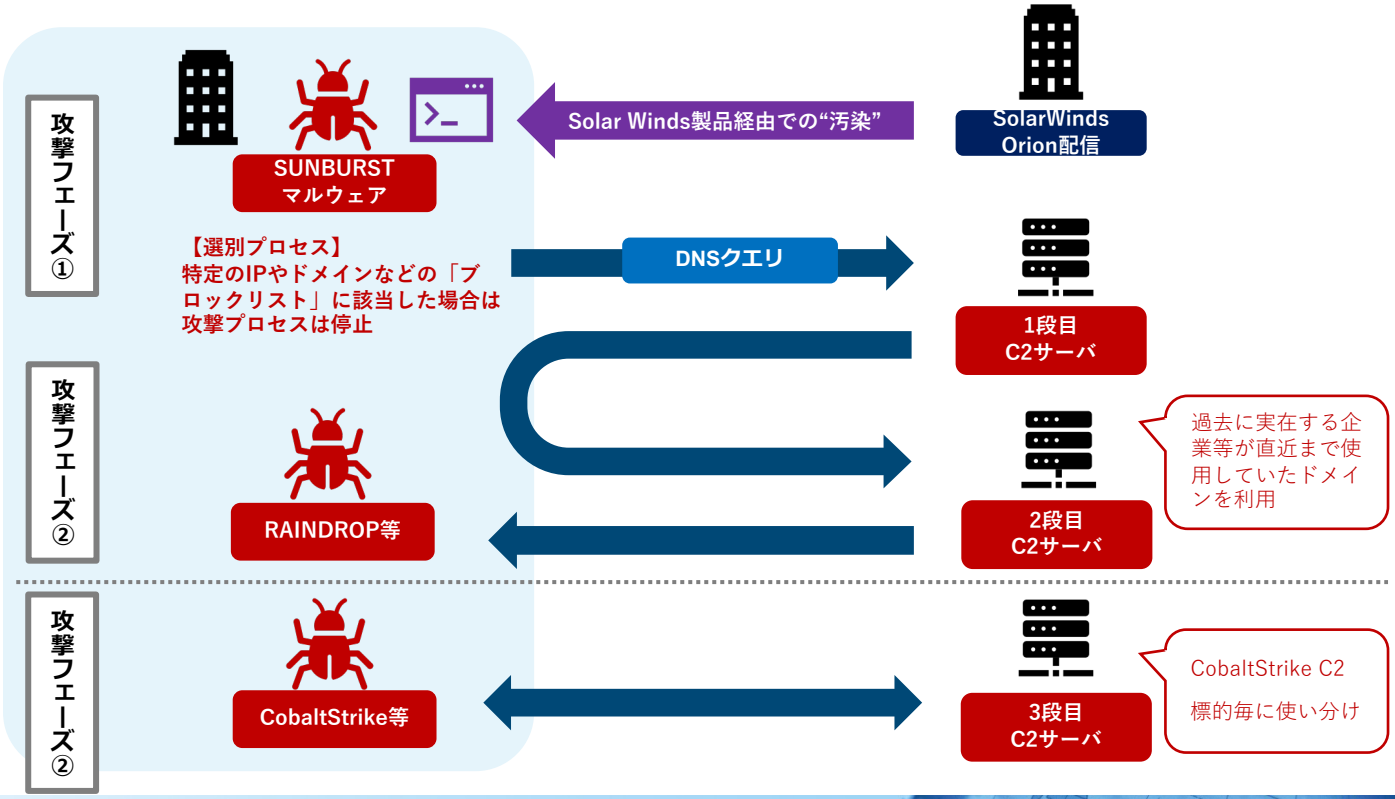


アトリビューションに必要な「時間」



Solarwinds事案：徹底したTTP重複回避

- 過去の多くのサイバー攻撃グループのTTPと共通点が見当たらず



Solarwinds事案：他グループとの関連性

- Solarwinds事案で侵害（1st Stage）された企業で観測された別？の攻撃キャンペーン（SilverFish）
  - Solarwinds事案の2nd Stage C2サーバと同じ共通点のあるＣ２サーバ群
  - 複数のオペレータチームが分担して大規模な攻撃インフラを管理
  - 使用していた攻撃インフラが、Trickbotと共通であったり、TTPがEvil Corpと類似しているとコメント（詳細はレポートに示されず）

  https://www.prodaft.com/resource/detail/silverfish-global-cyber-espionage-campaign-case-report
- SUNBURSTマルウェアと「Kazuar」マルウェアとの類似点について（Kaspersky社調べ）
  - 攻撃グループTurlaが使用しているKazuarマルウェアと共通点が見られた
  - 偽旗作戦の可能性も否定しきれないが、Kazuarマルウェア自体は2020年11月になり大幅にコード変更を実施しており、Solarwinds事案の発覚により共通点を知られないように急遽変更を行った可能性を指摘

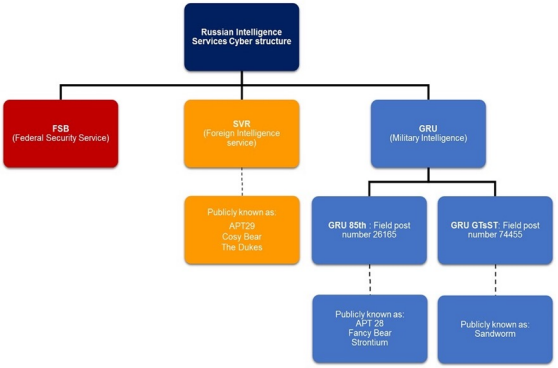
  https://securelist.com/sunburst-backdoor-kazuar/99981/

Solarwinds事案：他グループとの関連性

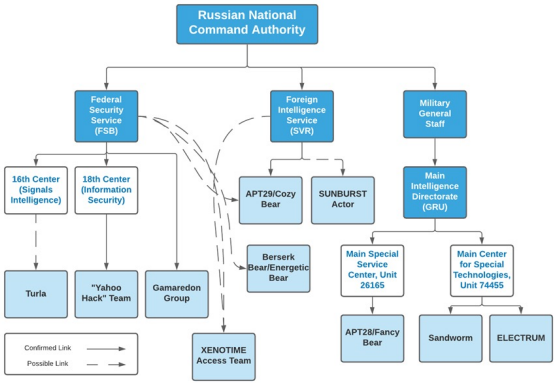
- 2020年7月に米CISA、英NCSC、加CSEが共同でAPT29に関する注意喚起を実施
  - 2020年にAPT29がCovid-19関連情報を狙う攻撃キャンペーンを行っていると指摘
  - Wellmessマルウェア等が使用されたと指摘
  - Wellmessは2018年にJPCERT/CC、ラックが分析レポートを発表したが、当時使用された検体と攻撃インフラについては、APT28との関係性がその後指摘された

英NCSC（2020年7月）
https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development
LAC（2018年6月）
https://www.lac.co.jp/lacwatch/pdf/20180614_cecreport_vol3.pdf
JPCERT/CC（2018年6月）
https://blogs.jpcert.or.jp/ja/2018/06/wellmess.html
Cisco TALOS（2020年8月）
https://blog.talosintelligence.com/2020/08/attribution-puzzle.html

「APT29」のグルーピングについて



https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise



https://twitter.com/jfslowik/status/1377026120931889152

- Domaintools社が、報道が「APT29」と伝えるときに、「SVRのサイバー活動」の意味で「APT29」という名称を使っている可能性について触れ、不正確である旨を指摘

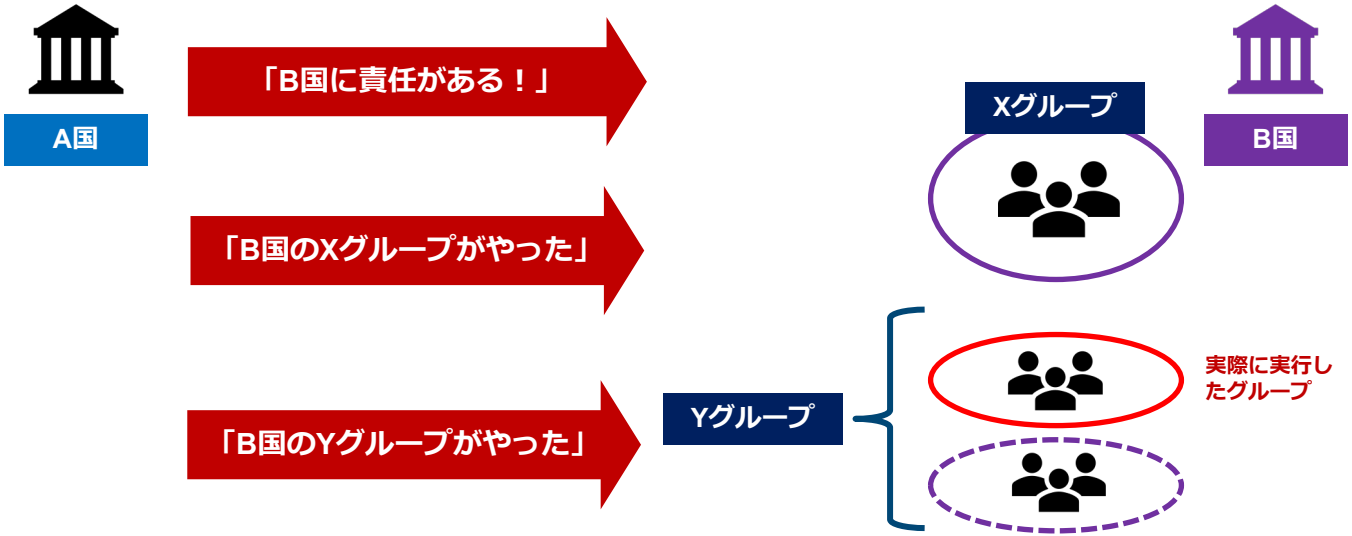
https://www.domaintools.com/resources/blog/continuous-eruption-further-analysis-of-the-solarwinds-supply-incident

- F-Secure社アナリストは、少なくともCosmicDukeについては複数のチームが使用していた可能性がある旨を指摘している（※2015年の古い記事）

https://blog.f-secure.com/ja/podcast-dukes-apt29/

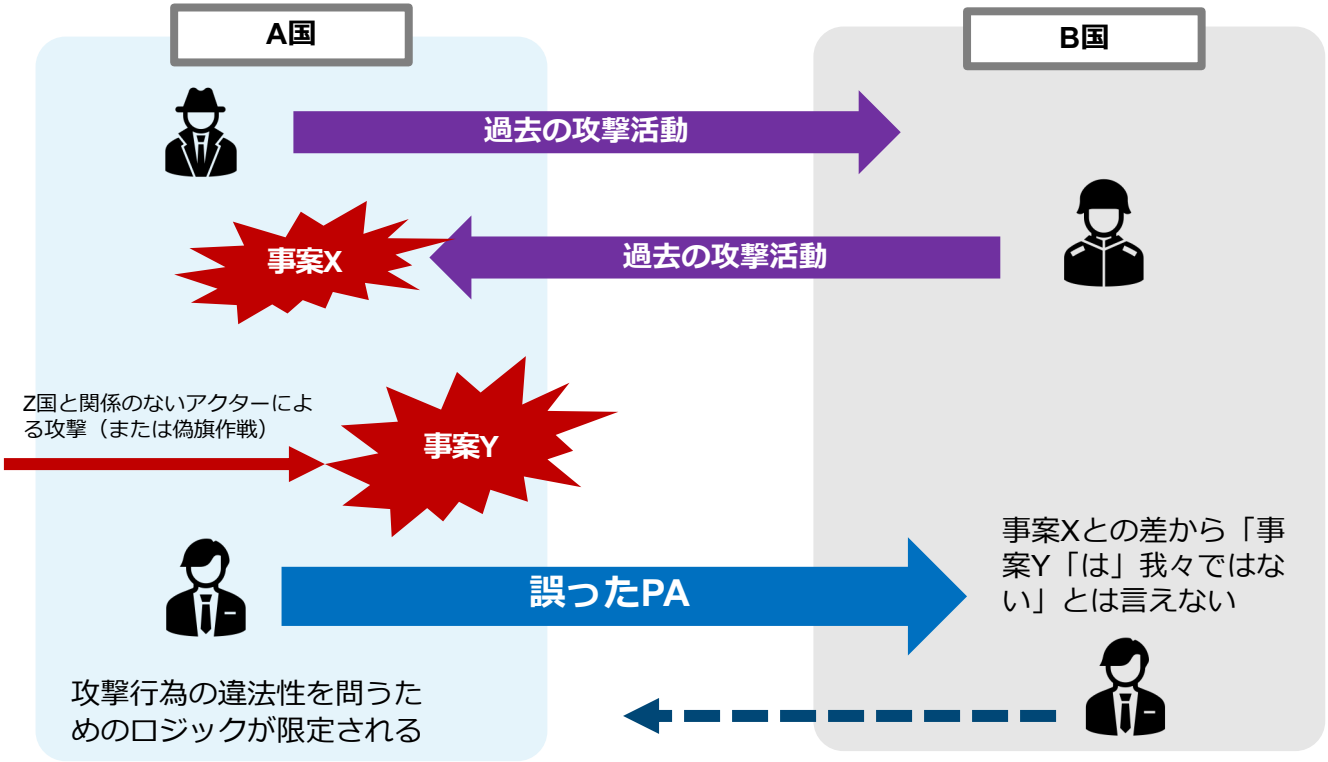
グルーピングの精度はどこまで問われるか

- 果たして、正確なグルーピングとアトリビューションの効果は関係するのか
- 非難が「大枠であっていればよい？」のか



パブリックアトリビューションのジレンマ

- お互いに「過去」のある者同士では効果がないのではないか？



米刑事訴追公表と技術情報公開の時間差（※作成中）

	攻撃時期	PA／経済制裁	刑事訴追	US-CERTほか	民間レポート
2014年5月 APT1訴追	2008年～2012年		2014年5月		2013年2月ほか多数
2014年11月 SPE事案	2014年11月前後	2015年1月 制裁指定	2018年9月	2014年12月19日 ※FBI FLASHは12月2日	事案発生直後 トレンドマイクロ：12月4日
Yahooメール侵害事案	2014年1月～		2017年3月		
Boyusec（APT3）刑事訴追	2011年～2017年5月		2017年11月		2014年以降多数
Mabna Institute事案	2013年～2017年12月	制裁指定	2018年3月	2018年3月	2018年8月 ※その後活動は継続
大統領選介入①	2016年	制裁指定	2018年3月		
大統領選介入②	2016年	制裁指定	2018年7月	2016年12月	CrowdStrike：2016年6月14日
Wannacry事案、SPE事案ほか	Wannacry事案：2017年5月	制裁指定	2018年9月	Wannacry：事案発生直後	事案発生直後多数
OPCW、スポーツ団体事案	2014年～2018年5月	制裁指定	2018年10月	2018年10月 英NCSC等	？
Turbine Panda事案	2010年～2015年5月		2018年10月		事案発生後に少数のレポート
APT10	2006年～2018年		2018年12月		事案発生後多数
Anthem事案	2014年10月～ ※公表は翌年2月		2019年5月		関連レポート多数
Equifax事案	2017年9月		2020年1月		
Chinachopper事案			2020年7月		関連レポート多数
APT41刑事訴追	2014年～		2020年9月		事案発生後多数
Sandworm刑事訴追	2015年～		2020年10月	多数（※）	事案発生後多数
RGB要員刑事訴追	2014年～	制裁指定	2021年2月	多数（※）	事案発生後多数
APT40刑事訴追			2021年7月	2021年7月	事案発生後多数