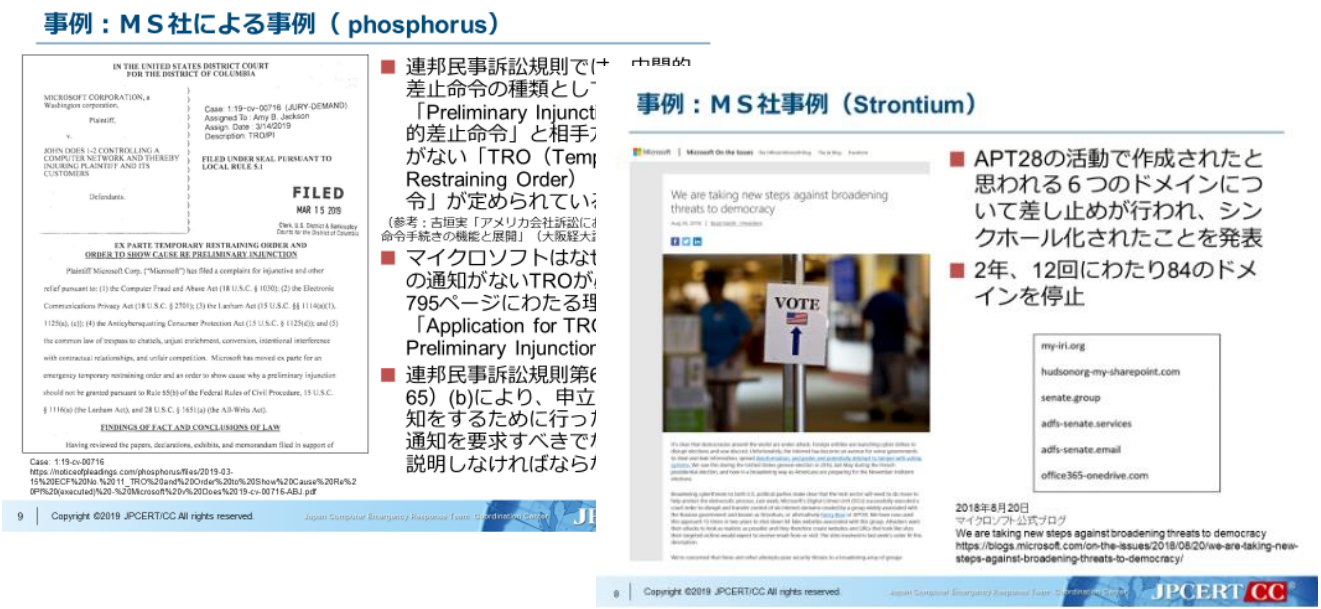
コーディネーションの現場からの視点

2021年1月28日

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

JANOG45での発表

- 「民事手続きを活用した攻撃インフラのテイクダウンに向けて」というテーマで発表
- 米マイクロソフト社がこれまでに行った、米連邦地裁における民事手続きによる、標的型サイバー攻撃やボットネットの攻撃インフラ（C2サーバーのドメイン）の差止手続き事例について紹介



2019年度調査について

- 主に米マイクロソフト社がこれまでに行った、民事手続きを用いた不正ドメインのテイクダウン事例について調査を行い、「必要な法的手続き」「期間」「コスト」などについて整理を行った

- 他のアプローチ方法（UDRP：統一ドメイン名紛争処理方針）などとの比較を行い、日本国内の民間主体が民事手続きを活用し得る可能性についてフィージビリティ調査を法律事務所のご協力により実施した

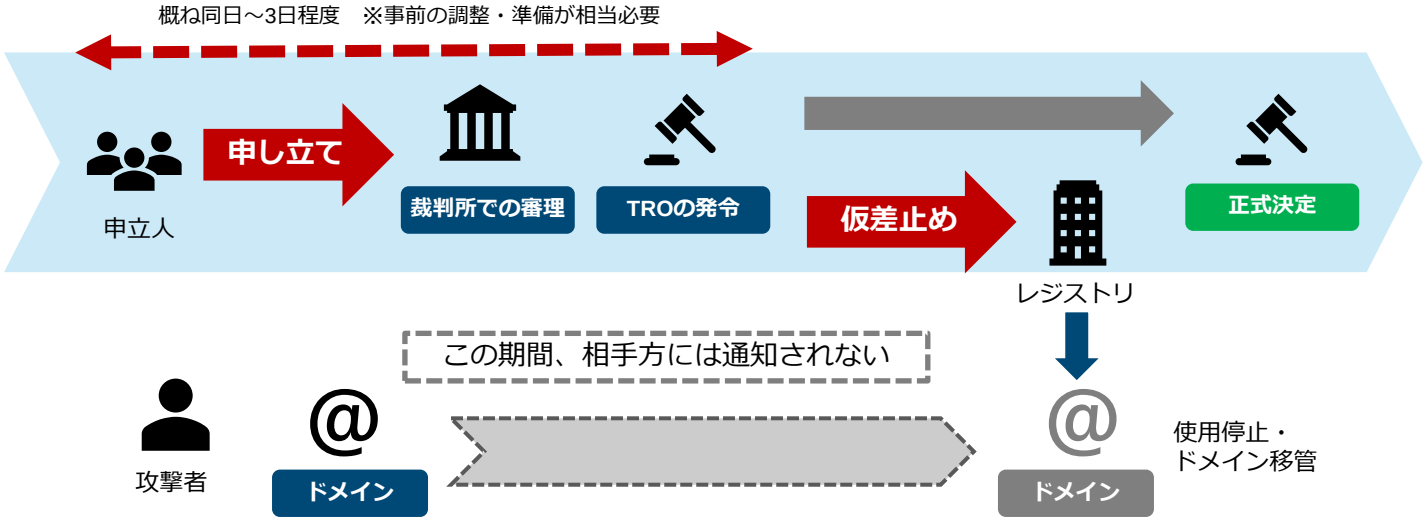
2019年度法律調査結果

メリット

- TRO（Temporary Restraining Order、仮制止命令）：短期間で秘匿性のある対処が可能
- 匿名の被告に対する請求が可能（John Doe訴訟）
- 請求対象が「商標類似」ドメイン名に限定されず、また請求主体も不正利用された者に限らない

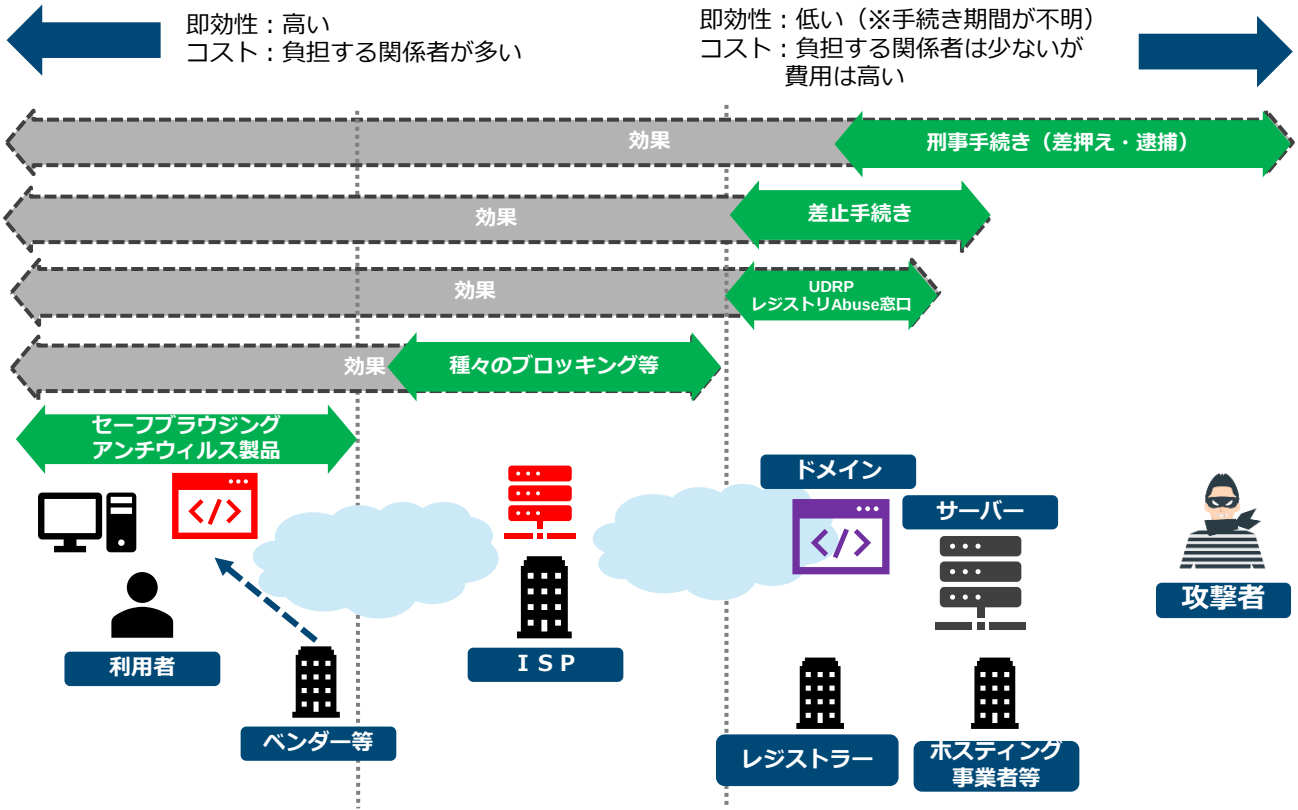
デメリット

- 発令要件（基本要件に加えて、急迫かつ回復不能の被害が生じることが明白、相手方への通知すべきでない理由など）のハードルが高い
- 手続きが複雑であり（ノウハウを有する）弁護士費用が高額になることが予想される
- 提訴できる連邦地方裁判所が限定される



さまざまな対処による複合的なアプローチ

JANOG45発表
資料の再掲



テイクダウンに向けた調整上の課題

- JPCERT/CCから国内外の事業者へ行っているのは「任意の依頼」
- 全体としてはAbuse対応いただける事業者は増えてきている印象だが・・・

- **①相手先により対応がまちまち**

・・・すぐに応じてくれるホスティング事業者やレジストラーもいれば、まったく対応してくれないところもある（理由はさまざま）。

①-(a)：「法的な手続き／処分をちゃんとしてくれ」と要求されるケース（裁判所の令状など）

①-(b)：調整時点で外形的に不正行為が確認できない限り止められない、と断られるケース（認知当時の不正コンテンツのコピーや関連ログが必要なケース）

- **②時間的な課題**

・・・フィッシングであれば48時間くらいで“使い捨て”されるため、そもそも（被害防止に）間に合わない

- **③“もぐらたたき”**

・・・ホスティング側で落としたとしても、同じドメインが別のIPアドレスで復活するケースや、ドメイン側を止められても、ホスティング側で落とせないと、別ドメインで復活するケースも

“共通言語”の必要性

- 調整先となる各事業者において、地域毎、事業毎に「止められない」事情はさまざま（法令や約款）
- 単に「不正なものだから止めてくれ」だけでは足らず、事業者が「合法的に（利用者との）契約を停止できる」ための“ロジック”や証拠が必要

- 取得の容易性が攻撃者側の優位性（低コストでの攻撃インフラ取得）につながるものの、ユーザー獲得のための企業努力との兼ね合いでもある
- 一律な審査の厳格化などを課すのは現実的ではないのではないか。不正契約者を業界として弾く仕組みがまず試されるべきではないか。

対象インフラに応じたアプローチを選ぶ視点

視点１：攻撃インフラの稼働時間

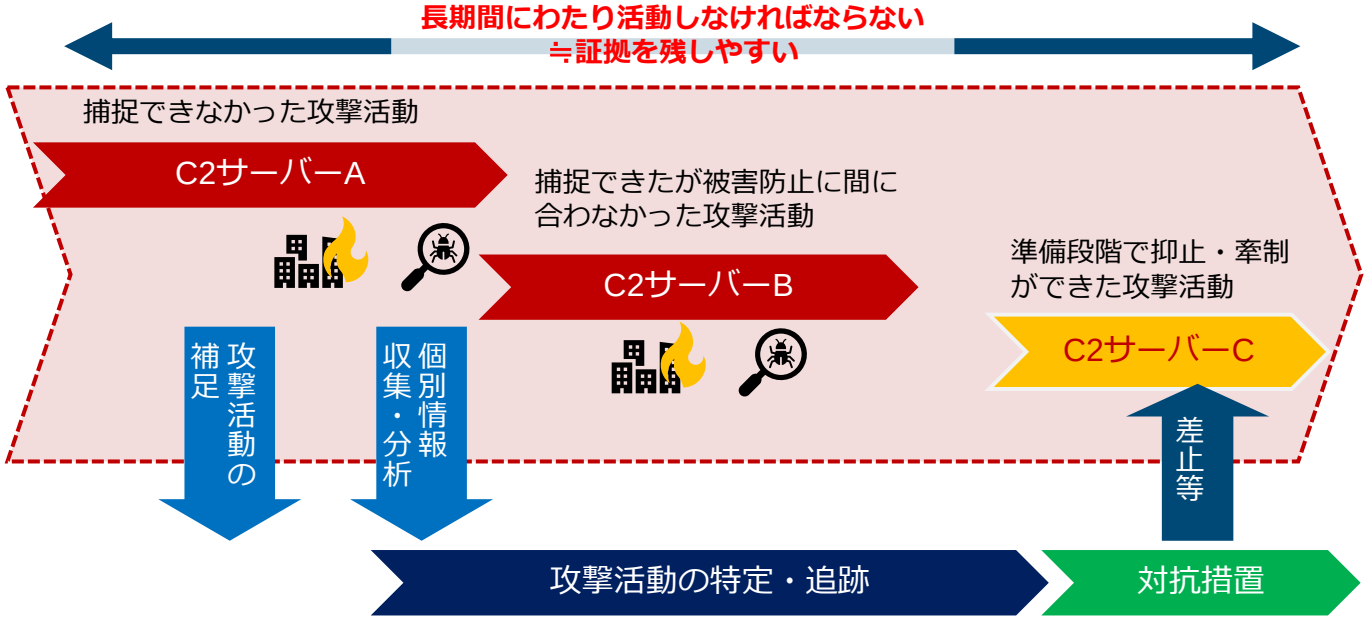
- 中長期的に稼働することで目的を達成するもの
  - 不正コンテンツの配信サーバー
  - 標的型サイバー攻撃のC2サーバー
- 短期間でも稼働することで目的を達成するもの
  - フィッシングサイト
  - 一時的な踏み台サーバー
  - ボット用の（中間）指令サーバー

視点２：テイクダウンコスト／時間

- 中長期間かかっても目的が達成できるもの
  - ボットネットテイクダウン
  - APTグループの刑事訴追
- 短期間に行わなくてはならないもの
  - フィッシング被害防止

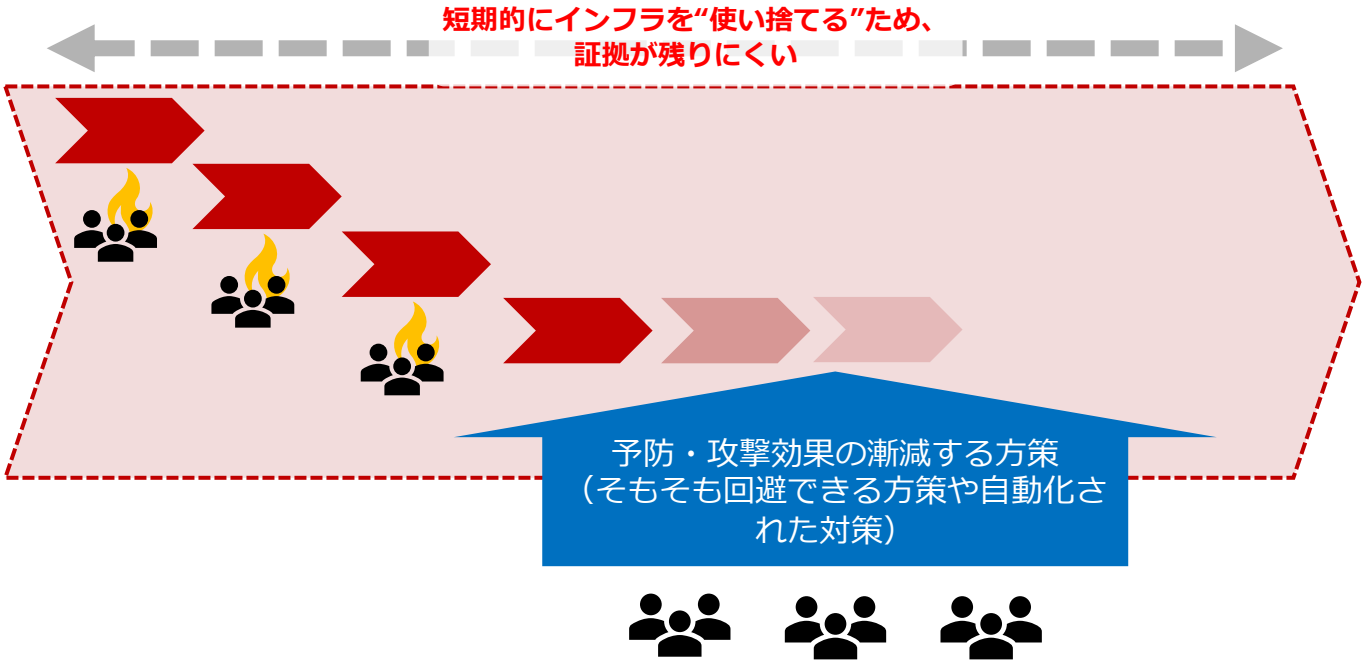
長期的なコストをかけるケース

- 標的型攻撃をはじめとする長期間にわたり活動しているケースでは、長期の対応（インシデント対応、調査・分析、情報共有）によって得られた情報が、その後の刑事訴追や差止などの対抗措置につながる
- 「今だ」というタイミングで強制的な手続きを行えるだけの「証拠」を収集しておかなければならない



短期的な対応が求められるケース

- 短期的にインフラを変える攻撃に対して対処することは手続き的に難しいため、「将来的に被害者になりうる利用者」に対する、予防策や被害軽減策を順次投入するほかない



お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- **Email：pr@jpcert.or.jp**
- **https://www.jpcert.or.jp/**

インシデント報告

- **Email：info@jpcert.or.jp**
- **https://www.jpcert.or.jp/form/**

制御システムインシデントの報告

- **Email：icsr-ir@jpcert.or.jp**
- **https://www.jpcert.or.jp/ics/ics-form.html**

※資料に記載の社名、製品名は各社の商標または登録商標です。