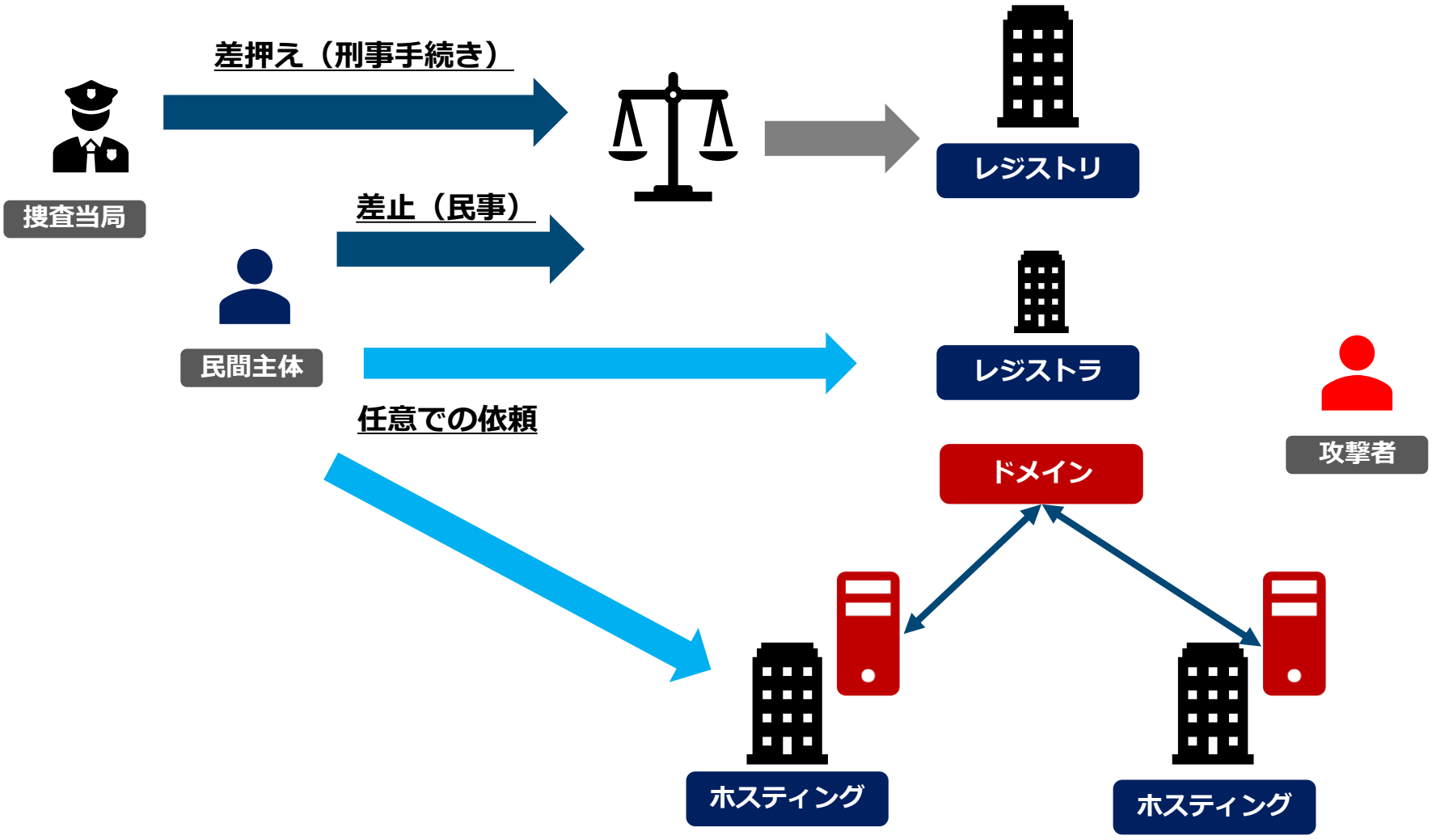
民事手続きを活用した攻撃インフラのテイクダウンに向けて

2020年1月23日
JPCERTコーディネーションセンター
早期警戒グループ　リーダー
佐々木　勇人

従前の不正ドメインのテイクダウン

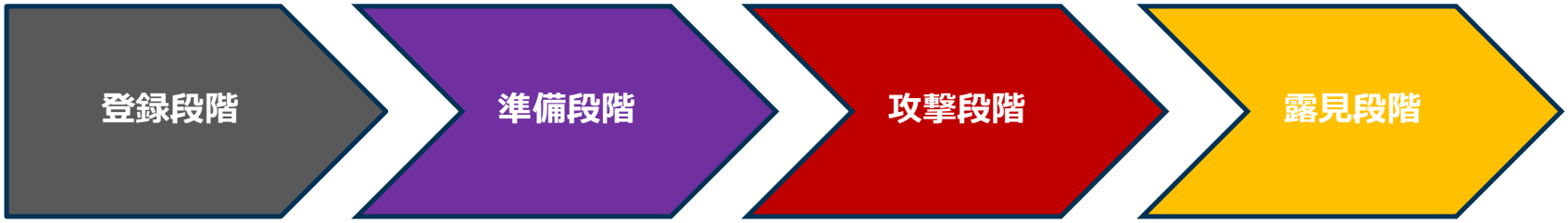


アジェンダ

- ドメイン差止め事例の紹介（マイクロソフト社の事例）
- ドメイン差止実績から見えるポイントについて
- 差止手続きに関するフィージビリティ調査について
- 質疑応答（ご意見お願いします！）

ドメインの利用サイクル毎のフェーズ

- 攻撃活動を抑止したり被害拡大防止のための早期対処において、攻撃者が用意・使用するドメインにいかにアプローチできるかが課題となっている。



<u>不正利用者問題</u>

虚偽の情報によるレジストラへの申込とドメイン取得

※攻撃者が攻撃インフラを用意している段階を検知することは困難

<u>ドメイン使い捨て問題</u>
（主にフィッシング）

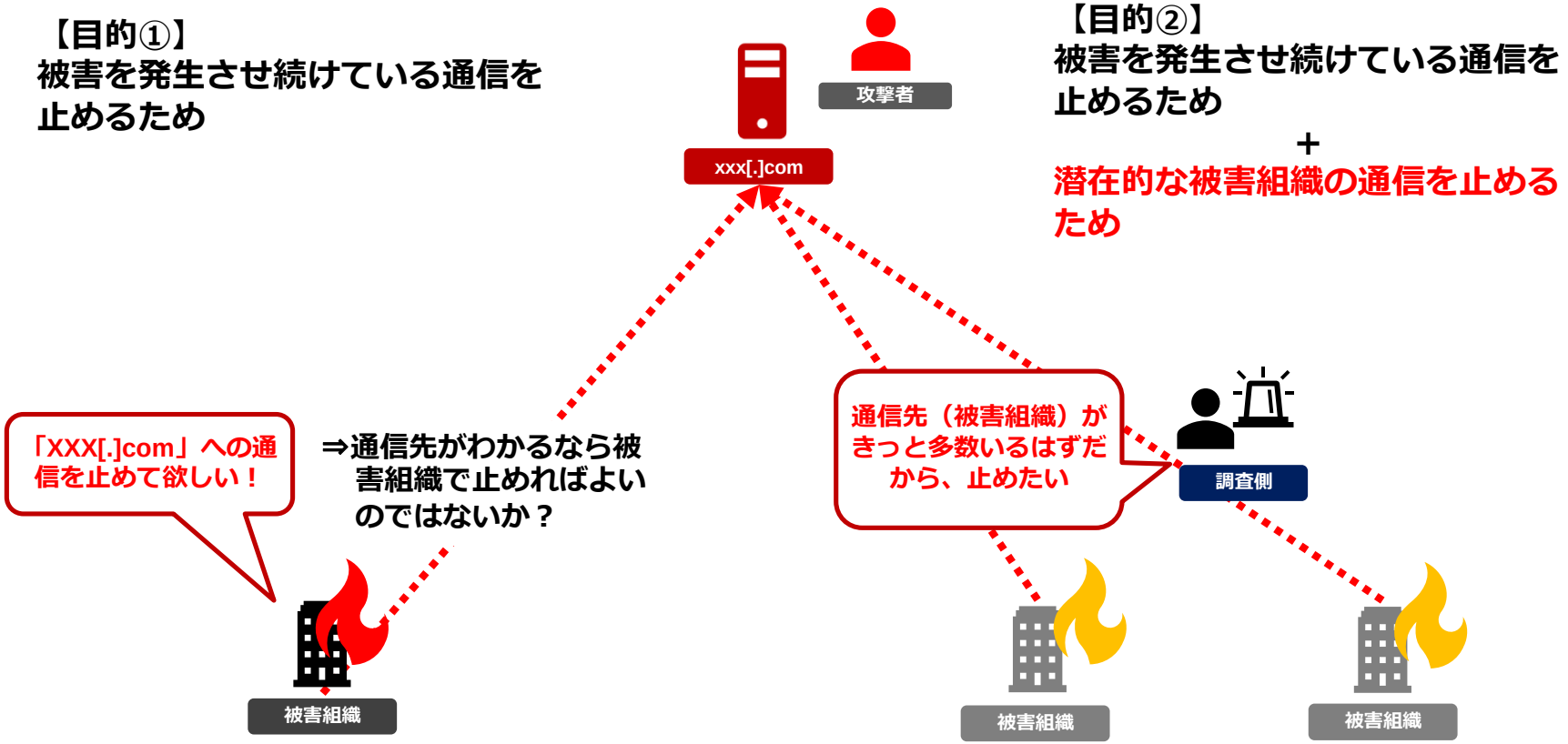
短期間でドメインを“使い捨てる”ため、通常のテイクダウン調整では対応が追い付かない

<u>サイトテイクダウンに係る課題</u>

サーバが所在していたホスティング事業者やプロバイダ側での対応には限界がある。

差し止める目的は何か

- 現在もなお被害を発生させ続けていることだけでなく、発生はしているが、被害を認識できない被害者（であり、調査（捜査）側も認識していない被害者）への通信を停止させることも含まれているのではないか。



マイクロソフト：民事手続きによる差止め実績

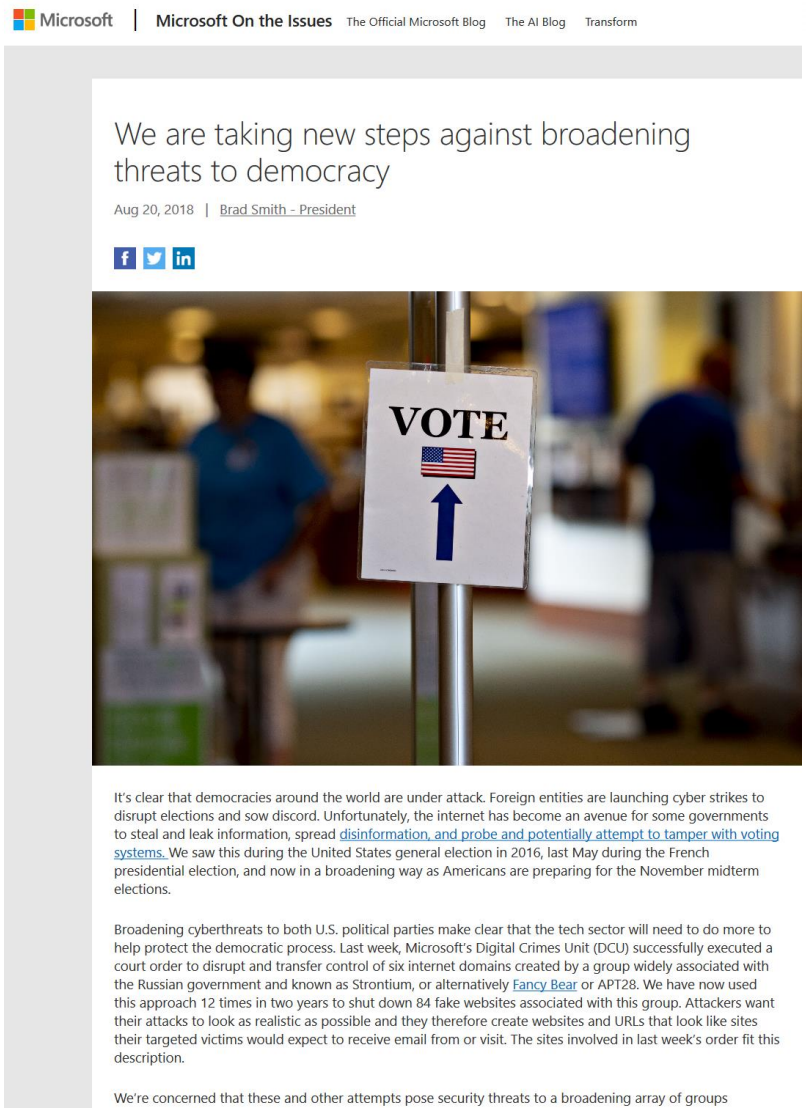
実施日	対象の攻撃活動（ボットネット、APT活動）	対象のgltdとレジストリ										その他
		.com Verisign	.net Verisign	.cc Verisign	.name Verisign	.info Afilias USA Afilias plc	.mobi Afilias	.biz Neustar	.us Neustar	.pro Afilias	.org Public Interest Registry	
2010年	Waledac	調査中										
2011年	Rustock	調査中										
2013年	Citadel	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	ほか各地域ドメイン多数
2013年	Zeroaccess	✓										ほかＩＳＰに対するもの多数
2013年	Bamital	✓	✓	✓		✓					✓	ほか地域ドメイン多数
2014年	shylock	✓	✓	✓				✓			✓	.su Technical Centor of Internet RIPN
2015年	Ramnit	✓										.IN
2017年	Dorknet	✓	✓			✓		✓				
2017年10月	Barium ⇒Shadowpad事案	✓										
2017年12月	Gamarue (Andromeda)	✓				✓						
2018年8月	Strontium	✓	✓								✓	
2019年3月	phosphorus	✓	✓		✓	✓	✓				✓	.BID .CLOUD .CLUB .PRO .NETWORK
2019年12月	Thallium	✓				✓	✓	✓			✓	.CASH .CLUB

事例：マイクロソフトによるドメイン差止申請

- 2019年3月27日マイクロソフトはイランのハッカーグループにより運用されていたとされる99のドメインの差止請求を行い、対象ドメインがマイクロソフトの管理下に移管された。
- TRO（Temporary Restraining Order）：仮制止（禁止）命令とPreliminary Injunction：予備的差止命令によりドメインの差止とドメイン移管（レジストリ（Verisign）による登録書き換え）が行われた

- 今回MSの代理人として手続きを担当したCrowell & Moring弁護士事務所のGabriel Ramsey弁護士はこれまでもWaledac、Citadel、Zeus、などのボットネットテイクダウンにも携わり、2018年のAPT28(ストロンチウム）関連ドメインの移管にも携わっている。

事例：ＭＳ社事例（Strontium）



Microsoft | Microsoft On the Issues The Official Microsoft Blog The AI Blog Transform

We are taking new steps against broadening threats to democracy

Aug 20, 2018 | Brad Smith - President

It's clear that democracies around the world are under attack. Foreign entities are launching cyber strikes to disrupt elections and sow discord. Unfortunately, the internet has become an avenue for some governments to steal and leak information, spread disinformation, and probe and potentially attempt to tamper with voting systems. We saw this during the United States general election in 2016, last May during the French presidential election, and now in a broadening way as Americans are preparing for the November midterm elections.

Broadening cyberthreats to both U.S. political parties make clear that the tech sector will need to do more to help protect the democratic process. Last week, Microsoft's Digital Crimes Unit (DCU) successfully executed a court order to disrupt and transfer control of six internet domains created by a group widely associated with the Russian government and known as Strontium, or alternatively Fancy Bear or APT28. We have now used this approach 12 times in two years to shut down 84 fake websites associated with this group. Attackers want their attacks to look as realistic as possible and they therefore create websites and URLs that look like sites their targeted victims would expect to receive email from or visit. The sites involved in last week's order fit this description.

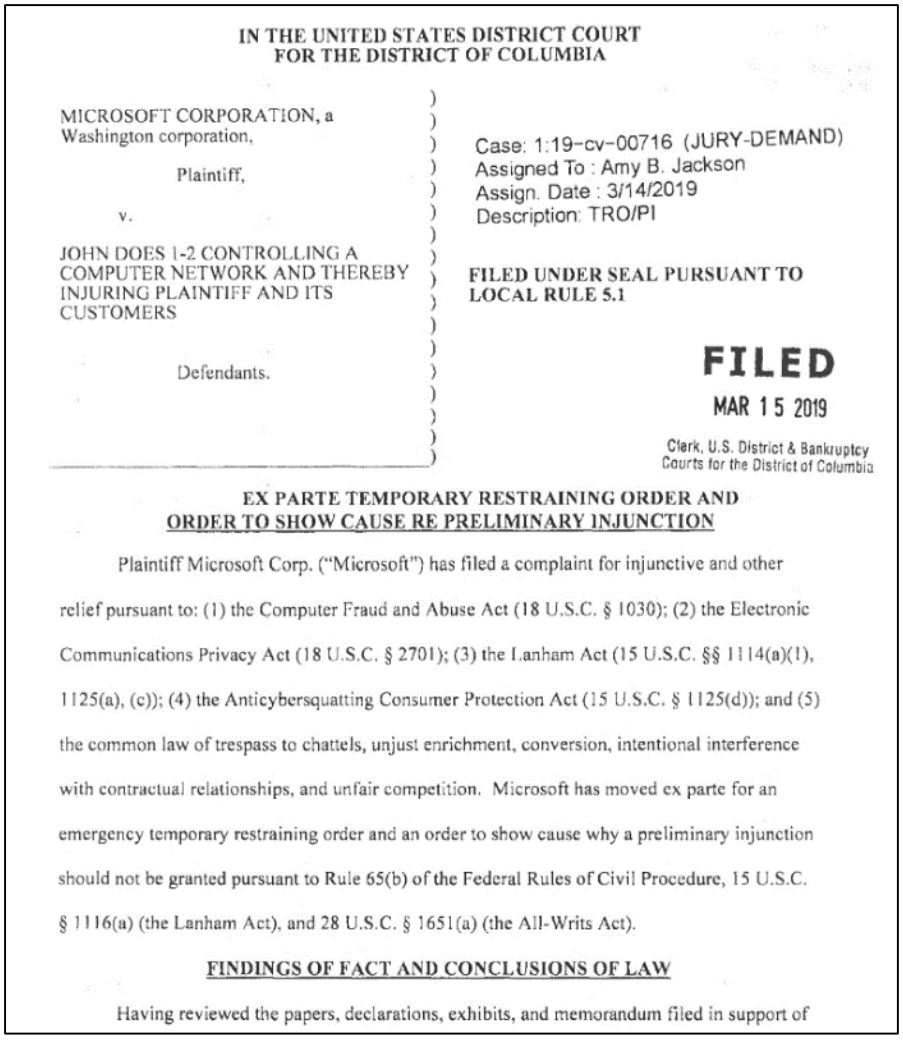
We're concerned that these and other attempts pose security threats to a broadening array of groups

- APT28の活動で作成されたと思われる６つのドメインについて差し止めが行われ、シンクホール化されたことを発表
- 2年、12回にわたり84のドメインを停止

my-iri.org
hudsonorg-my-sharepoint.com
senate.group
adfs-senate.services
adfs-senate.email
office365-onedrive.com

2018年8月20日
マイクロソフト公式ブログ
We are taking new steps against broadening threats to democracy
https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

事例：ＭＳ社による事例（ phosphorus）



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2 CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS

Defendants.

Case: 1:19-cv-00716 (JURY-DEMAND)
Assigned To : Amy B. Jackson
Assign. Date : 3/14/2019
Description: TRO/PI

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1

FILED
MAR 15 2019
Clerk, U.S. District & Bankruptcy Courts for the District of Columbia

EX PARTE TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corp. ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Electronic Communications Privacy Act (18 U.S.C. § 2701); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); (4) the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)); and (5) the common law of trespass to chattels, unjust enrichment, conversion, intentional interference with contractual relationships, and unfair competition. Microsoft has moved ex parte for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of

Case: 1:19-cv-00716
https://noticeofpleadings.com/phosphorus/files/2019-03-15%20ECF%20No.%2011_TRO%20and%20Order%20to%20Show%20Cause%20Re%20PI%20(executed)%20-%20Microsoft%20v%20Does%2019-cv-00716-ABJ.pdf

- 連邦民事訴訟規則では、中間的差止命令の種類として、「Preliminary Injunction：予備的差止命令」と相手方への通知がない「TRO（Temporary Restraining Order）：仮制止命令」が定められている。

（参考：吉垣実「アメリカ会社訴訟における中間的差止命令手続きの機能と展開」（大阪経大論集62巻4号）

- マイクロソフトはなぜ相手方への通知がないTROが必要なのか、795ページにわたる理由書「Application for TRO and Preliminary Injunction」を提出
- 連邦民事訴訟規則第65条（Rule 65）(b)により、申立代理人が通知をするために行った努力及び通知を要求すべきでない理由を説明しなければならない

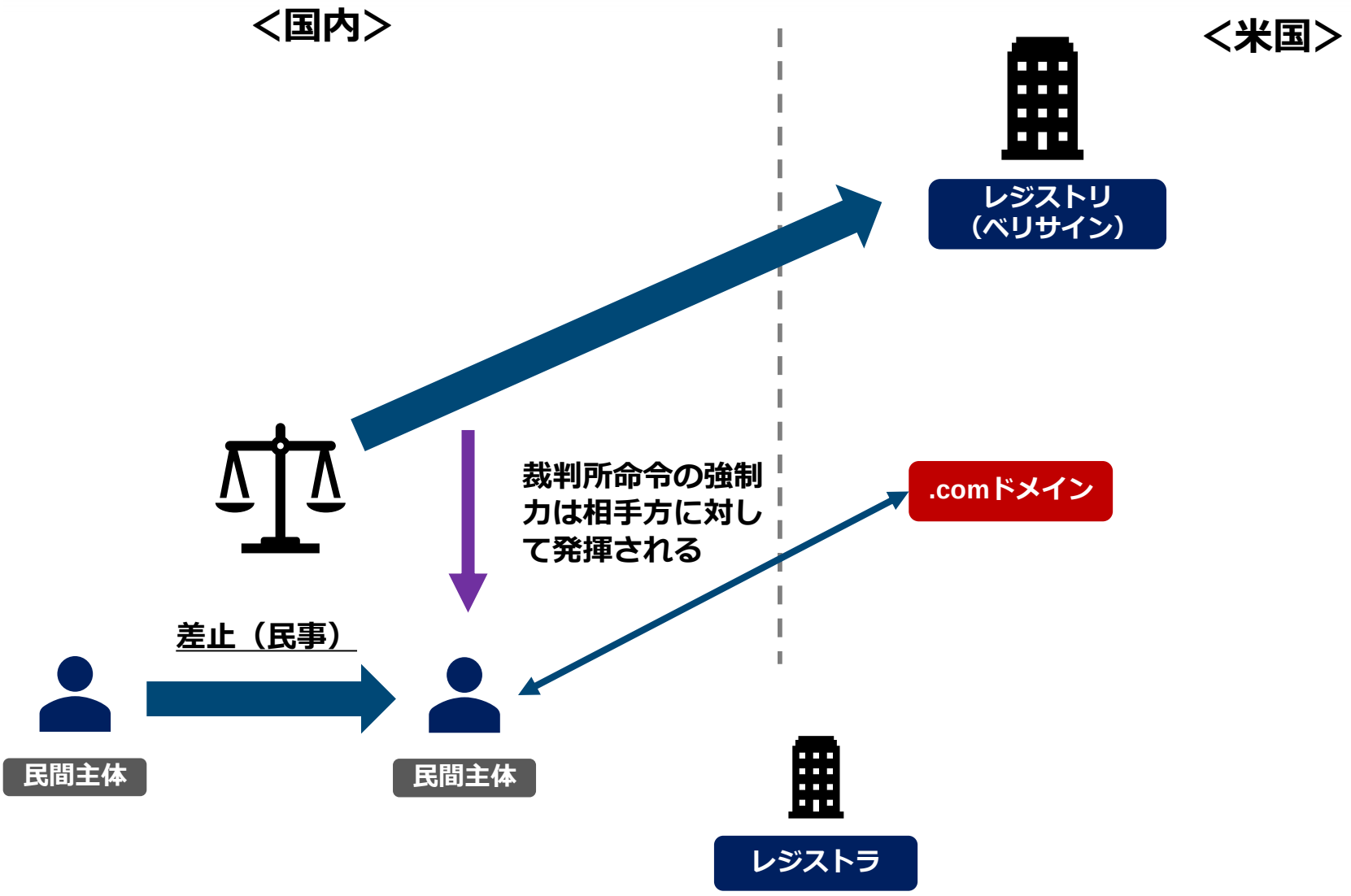
事例：ＭＳによる差止申請　Thallium

- （2019年12月の事例。国内向けの攻撃活動を含む（作成中））

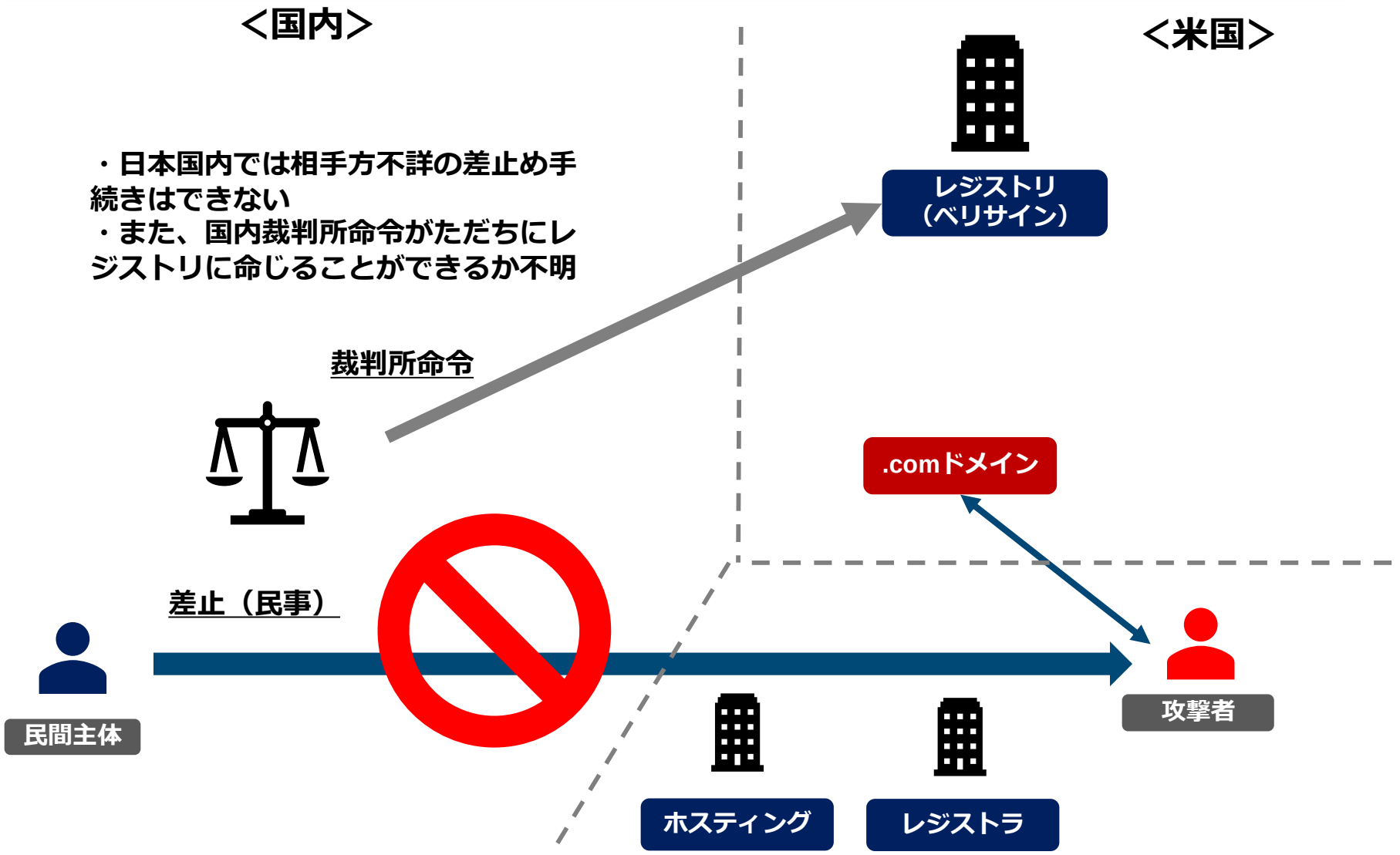
差止後にどのような処置を行うか

- （ネームサーバの変更とシンクホール化の手続きについて（作成中））

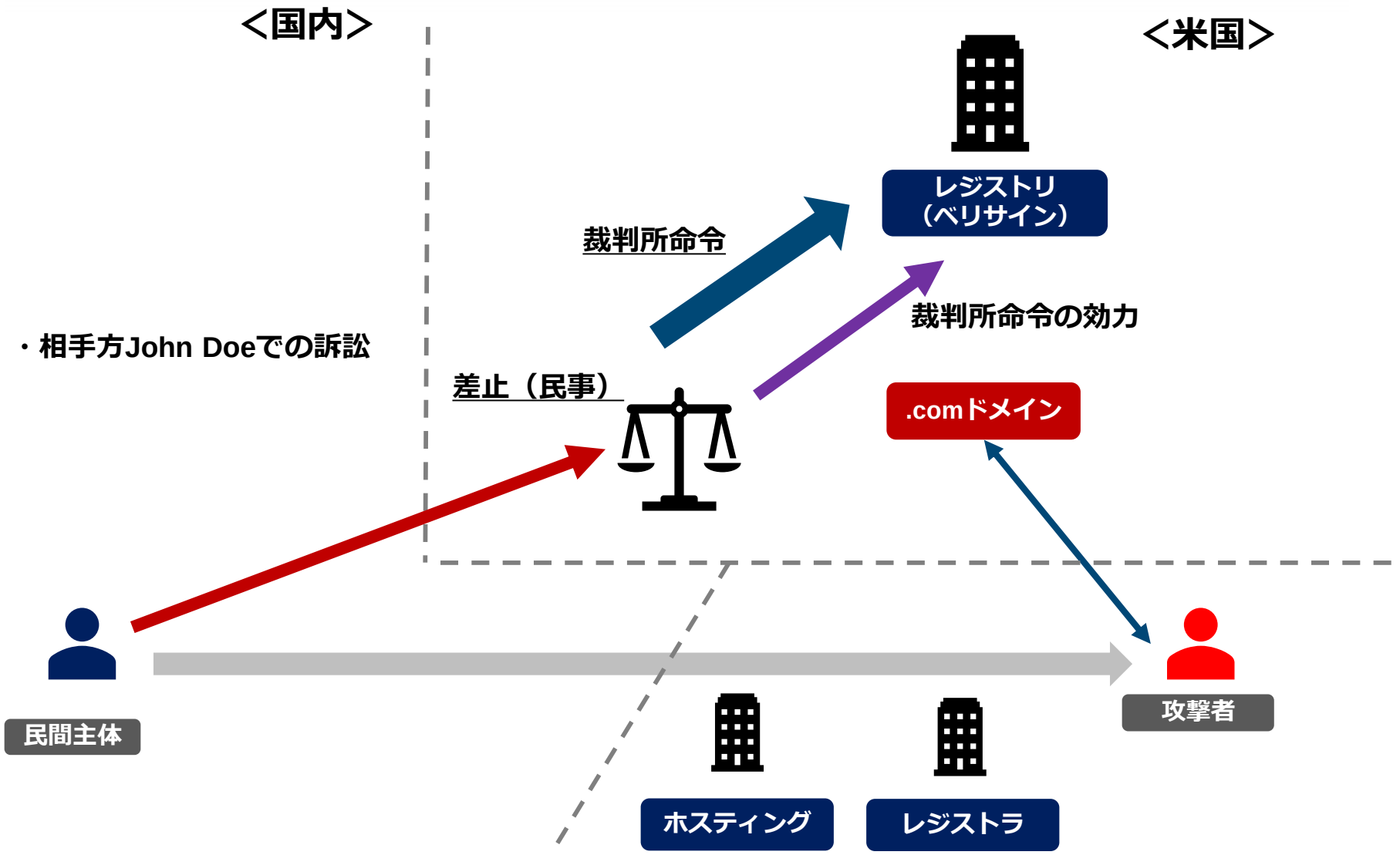
国内から手続きを行う場合①（相手方が判明）



国内から手続きを行う場合②（相手方が不明）



米国において手続きを行う場合（相手方が不明）



米国事例のぽいんと

- 過去10年内の差止め事例（ボットネットのインフラ、標的型攻撃のC2サーバに使用されていたドメイン）を踏まえると、**主に北米に拠点を置くレジストリに対して**裁判所命令を発出してもらい、差止実施とドメイン管理者の移管（とシンクホール化）を実施している。
- 米国においては、（物理的に）攻撃者不詳の状態においても「JohnDoe訴訟」が可能なため、攻撃に使用されたドメインを含む複数のドメイン登録を行った**登録者情報を特定**し、「特定の攻撃者」を手続きの相手方としている
- 米国においては、条件を満たせば、相手方（対象ドメインの既存の登録者＝攻撃者）への通知前に「TRO（Temporary Restraining Order）：仮制止命令」が発行され、差止が行われる

今後予定している調査について

- サイバー攻撃に用いられる不正ドメインを可能な限り被害が拡大する前段階において無効化する法的手段について、どのような手法があり得るか調査するとともに、実施可能性について検討を行う
- 調査対象の手段（案）

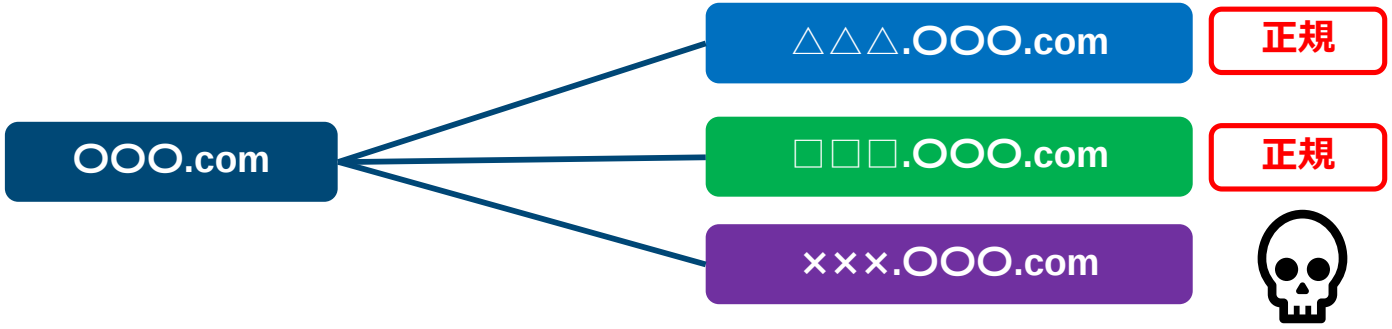
  候補①：日本国内の民間主体が米連邦地裁における差止請求を行う場合

  候補②：統一ドメイン紛争処理（UDRP）によるレジストラへの請求を行う場合

  候補③：（その他、候補となる法的手段がある場合）
- 上記候補のそれぞれの実施方法（必要な手続き、書面、コスト等）と他の候補との比較（メリット／デメリット）を調査・検討する。

今後予定している調査について

- 対象ドメインについて
  - .comドメインの場合
  - その他gLtdドメインについて（.net、.infoなど主要な２，３ドメインを選択の上対象とする）
- 個別に取得したドメインのほか、ダイナミックDNSサービスにて取得したドメインの場合についても、どのような方策がとり得るか検討を行う



- JPドメインについては、2019年10月から「JPRSにJPドメイン名の不正登録に関する情報受付窓口」を開設・運用を開始したため本検討対象外とする。
  https://jprs.jp/whatsnew/notice/2019/191002.html

今後予定している調査について

- 各法的手段において、以下の項目を調査・検討する

〇当該手段を実施できうる主体について

→例）当該対象不正ドメインの悪用による不利益を受ける主体でなければ申立することができない

〇必要な手続きの手順と期間

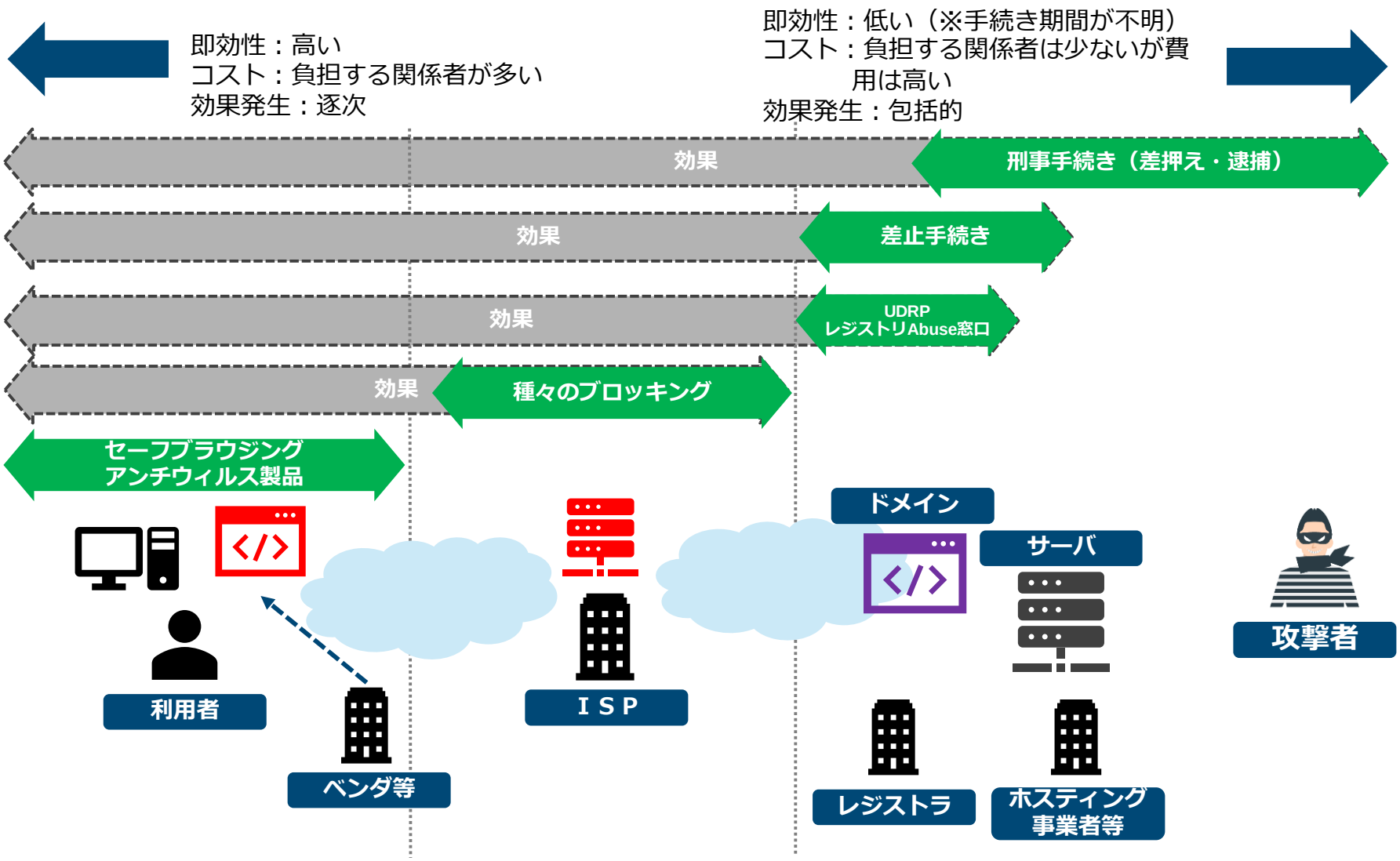
→どのような手順で手続きが必要であり、かかる手続き期間と実際に効力が発揮（ドメインのSuspendや廃止）されるまでの期間の想定について

〇必要なコスト

→申請手数料のほか、書面準備等に弁護士資格を持つ者の関与が必要な場合はかかる報酬等の費用も見込む

〇失効後、当該ドメインはどのような取扱いになるのか

不正ドメインに対する様々な対処方法の比較



お問合せ、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
- Tel：03-6271-8901
- 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