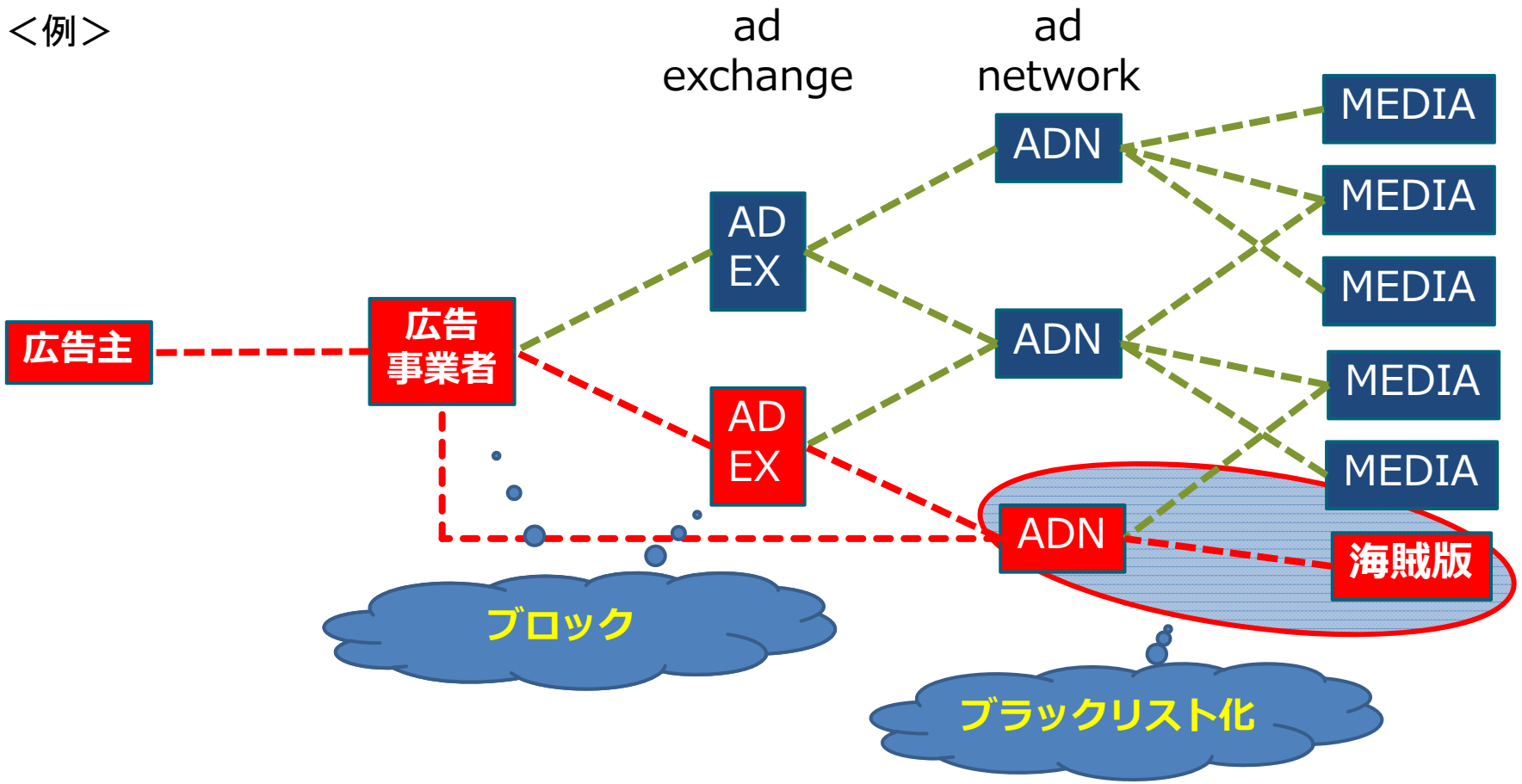
資料3

# 寺田眞治氏提出参考資料

# 違法サイトへの広告出稿は止められるのか？



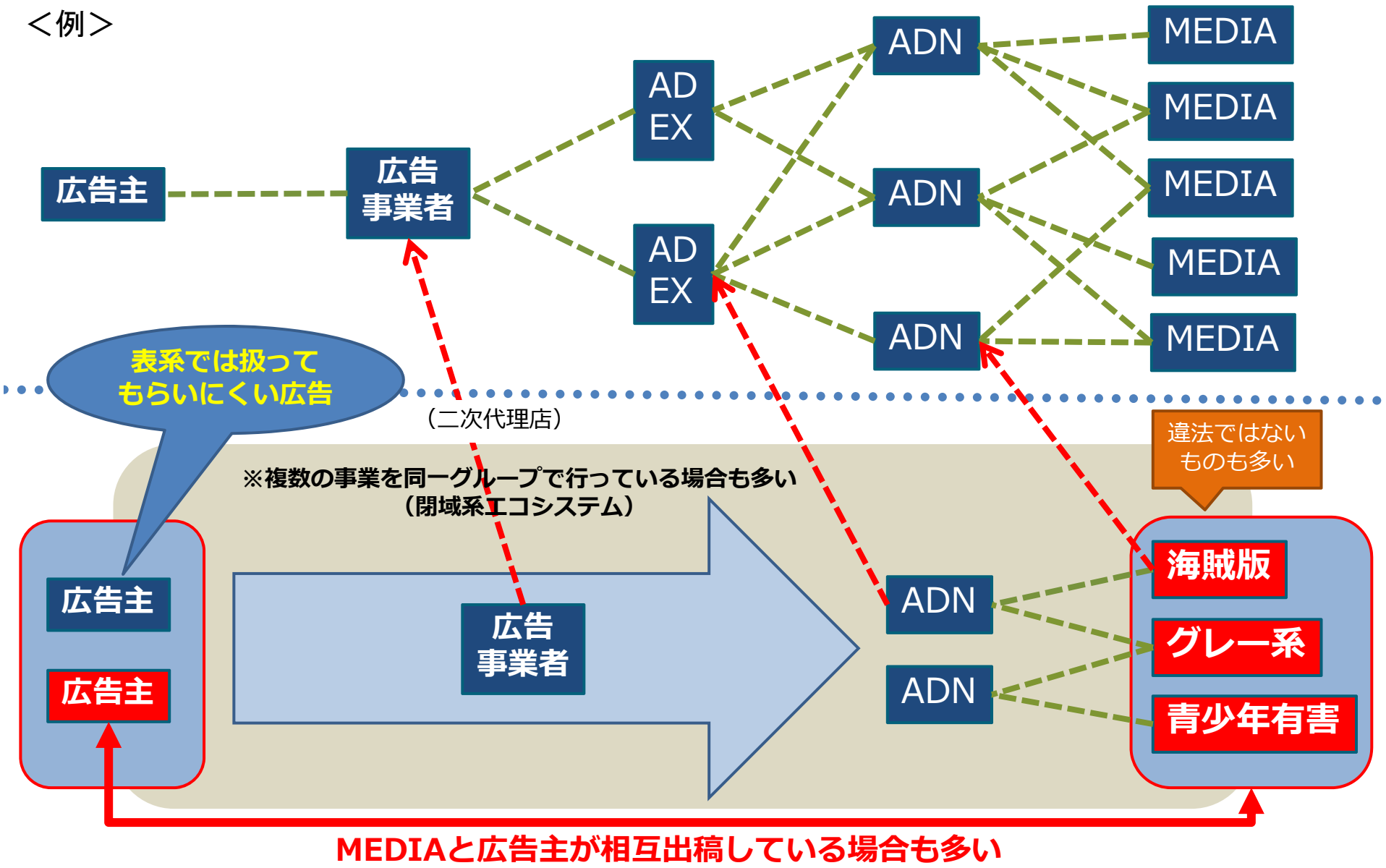

**広告出稿を止めることができるポイントは複数ある**

↓

**下流になるほど確信犯　→　ブラックリスト化して上流でブロック**

※海賊版サイトは広告収入が主であるため特定のADNとグルの場合が多い※

# 違法サイトへの広告出稿は止められるのか？



# 違法サイトへの広告出稿は止められるのか？

＜類型＞


・広告料の計算のため、広告がいつ、どこに掲載されたかについてはad networkは必ず把握している。
・広告料の支払いのため、ad networkは必ずmediaの振込口座を知っている。

・広告枠については、匿名の広告枠がある。
　→　知名度のあるmediaに集中してしまうことを避けるため。
　→　この場合、上流の事業者は掲載メディアがわからない。

**ad networkによる対策**
・メディア仕入れの際のチェックの徹底（契約事項の標準化）
・モニタリングの徹底（契約後のサイトやコンテンツの差し替え、アドフラウドの検知）
・違法、悪質サイト等の情報発信　→　共有化の仕組みが必要

＜類型＞


・どのad networkを通じて配信されたかは必ず把握している。
・広告料の支払いのため、ad exchangeは必ずad networkの振込口座を知っている。

・匿名の広告枠については、掲載メディアがわからない。
　→　ad networkを信頼するしかない

**ad exchangeによる対策**
・ad networkとの契約の際のチェックの徹底（契約事項の標準化）
・モニタリングの徹底（悪意のあるad networkの検知）
・悪意のあるad networkの情報発信　→　共有化の仕組みが必要

# アドフラウド（ad fraud）

一般社団法人 日本インタラクティブ広告協会による類型

**Ad Density（過度な広告領域）：** 検索スパムと組み合わせて、広告しかないページに誘導して広告アクセス増を図るもの。

**Ad Injection（不正な広告挿入）：** ユーザーが閲覧している正当な媒体ページの広告タグを、不正事業者（不正アドネットワークなど）が自社広告タグにすり換えることで、不正な収益を得るもの。

**Auto Refresh（過度に自動リロードされる広告）：** 高頻度で自動リロードを繰り返し、ごく短時間に大量の広告を表示させたりするもの。

**Cookie Stuffing（不正な成果の獲得のためのクッキー汚染）：** ユーザーブラウザにプレミアムメディアやブランド広告主のページをポップアップで表示させることで、ユーザーブラウザに優良な閲覧履歴のクッキーを生成させる手法。

**Falsely Represented（オークションの URL 偽装）：** アダルトコンテンツや違法ダウンロードの事業者が、広告オークションに対して、正当なサイトの URLを偽装して、広告の入札を受けようとする手法。

**Hidden Ads（隠し広告）：** ブログパーツの見えない領域に広告を仕込んだり、CSS 等でユーザーに見えない形で広告を配信したりすることで、広告配信数を水増しするもの。

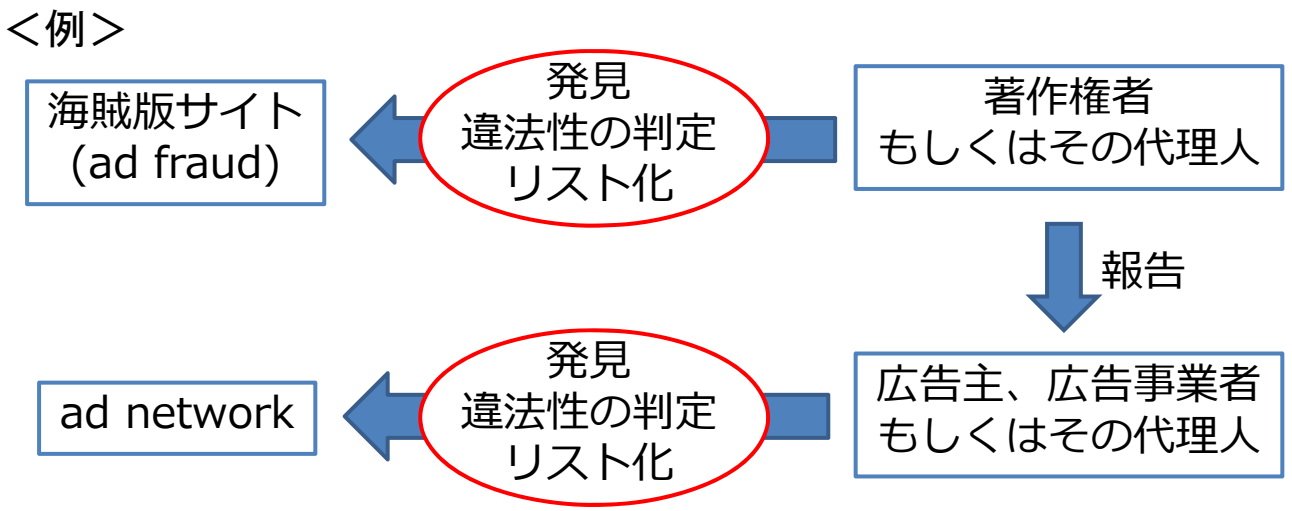
**Imp/Click Bot, Retargeting Fraud（プログラムされたブラウザによる広告閲覧）：** ブラウザをプログラミングして、自動的に imp、クリックを発生させる手法。

**Malware, Adware, Hijacked Device（支配権を奪われた個人端末からの広告リクエスト）：** ユーザーデバイスを不正プログラムに感染させ、自社サイトの広告を閲覧させたり、クリックさせたりするもの。

**Sourced Traffic（By Traffic Exchange、トラフィックエクスチェンジ）：** ユーザーにページ内の自動リロードのコンテンツを閲覧させ、コンテンツ元にトラフィックを渡して対価を得るもの。

**AIによりad fraudを検知するツール → ブラックリストの作成と配信制御の可能性**

# 課題

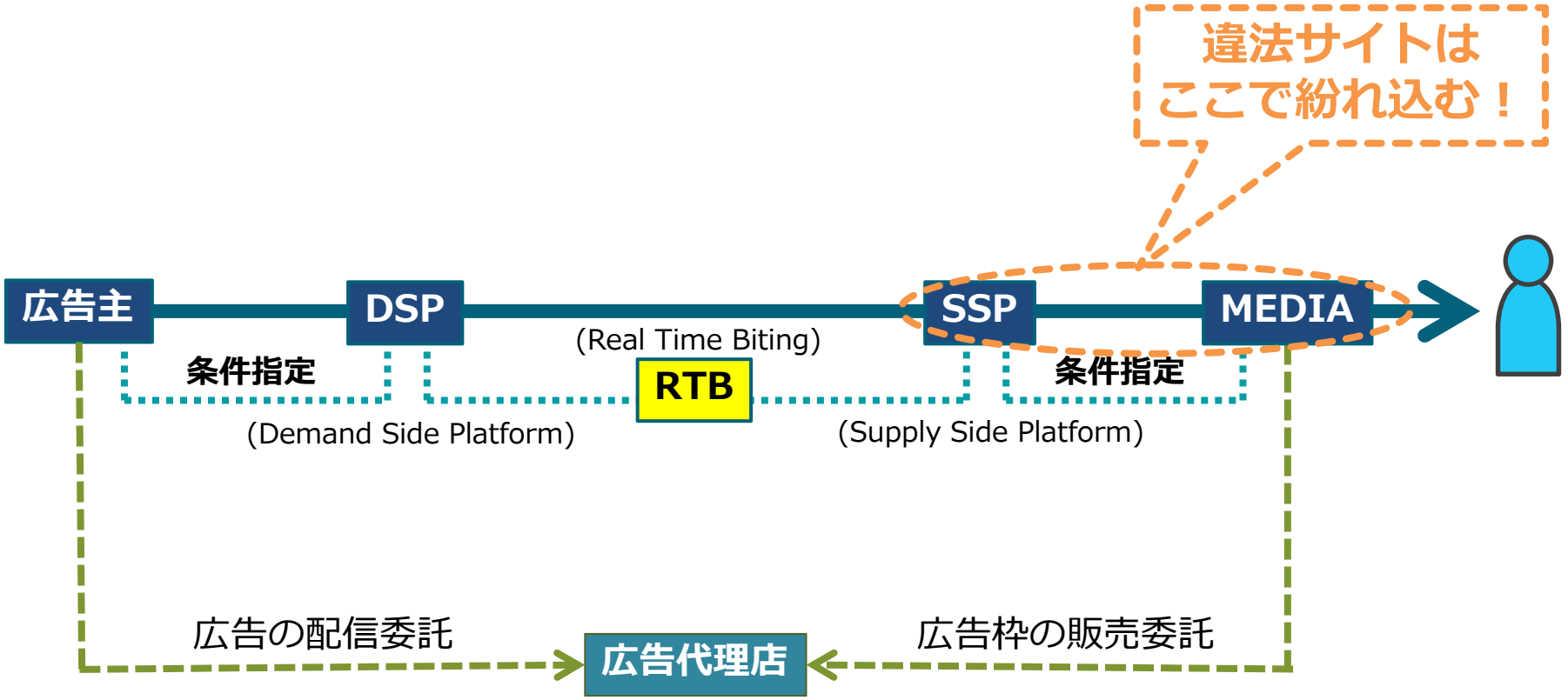



| | | | |
|---|---|---|---|
| 主な課題 | 発見するためのコスト<br>違法性の判断基準と判定者の選定<br>リスト管理（メンテとコスト）<br>インセンティブとエンフォースメント | ⇔ | 当事者がすべきなのか<br>第三者が介在すべきなのか |

**独自の裏社会（必ずしも違法とは限らない）に対しては効果がない。。。**

# （参考）オンライン広告配信の仕組み（RTBの例）

①ターゲットに合致する来訪者がメディアを訪れた場合、空き枠であればSSPを通じて広告主側のDSPに通知。
②広告主はDSPにあらかじめ入札金額等の条件をメディア毎に設定してあり、DSPとSSPの間で、リアルタイムで条件交渉が行われ、入札金額が一番高いDSPが配信。



# （参考メモ）

・近年、広告主にとっても広告配信先の把握が難しくなる中、広告主が侵害サイトに出稿しないことは、どの程度、技術的に可能か。

→ ad network絡みは技術的には可能だが、悪意のあるmedia、ad network、ad exchangeを排除できるのはそれぞれの上位レイヤー事業者の取り組み次第であり、これを裏付け支援するモニタリングと情報共有の仕組みが必要。
→ ad fraudの排除については、技術的に完全な方法はなく、広告主を含む業界全体で、意識の向上、技術の向上、情報共有の仕組み構築等が必要で、自主的取り組みだけでなく、ネット業界全体としての支援も考えられる。

・現在の取組に加えて、侵害サイトへの広告出稿の抑制を更に効果的に実施するには、どのような追加的な方策があり得るか。

→ 基本は業界の自主的取り組みだが、著作権者に対するモニタリング、情報共有等について支援は考えられる。また、広告主や消費者への啓発も間接的ではあるが効果はある。

・海外の広告主や、日本企業であってもJAA・JAAA・JIAAのような業界団体に加わっていない広告主もいる中、広告団体の侵害サイトへの出稿抑制により、どの程度、侵害サイトへの収入を抑制することが可能か。

→ いわゆる表の世界からの資金流入は、ほぼ抑制できるが、一方でグレーゾーンは全くの別世界であり、過去から連綿と継続し、今後も存在し続ける。（明確な違法性が無ければmedia、広告事業者だけでなく広告主も排除することはできない）

・諸外国の経験を踏まえて、日本が学ぶべき取組、諸外国との協力の可能性等があるか。

→ 欧米先進国に比べ、日本は発展状況も対応状況も遅れる傾向がある。したがって、放っておいても問題発生後に自主的な対応が進むというパターンであるが、現実的に政府や官公庁が介入するのは、広告業界の進展スピード、表現の自由問題等で困難である。