DNSブロッキング

やまぐち@IIJ

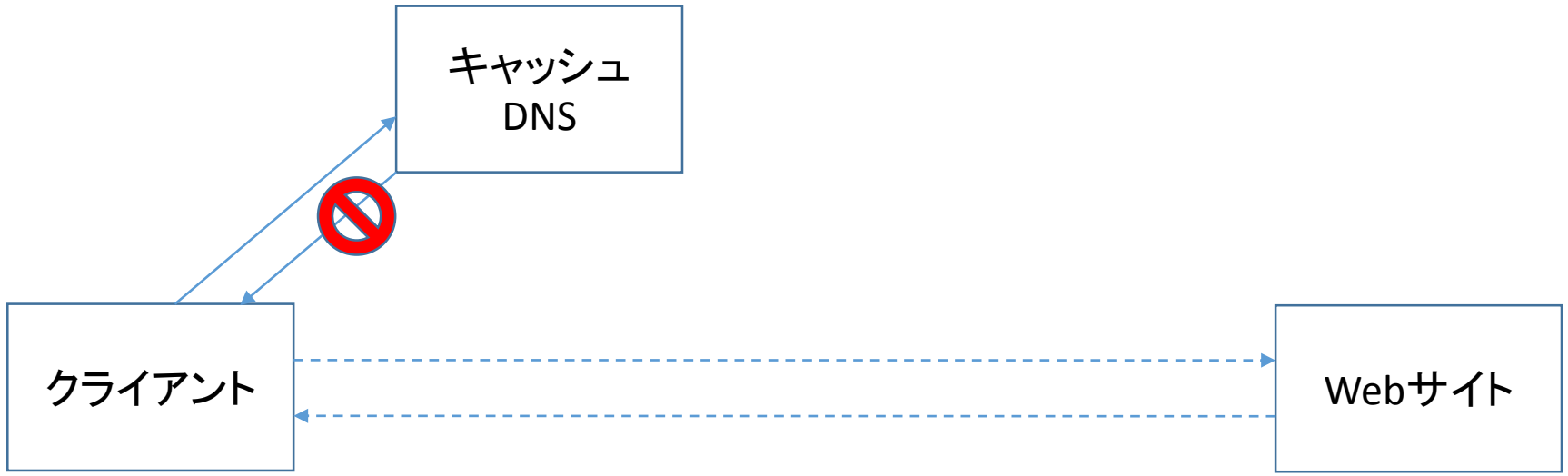
ブロッキングとは

- ユーザの同意を得ずにすべての通信を監視し、特定サイトへのアクセスであれば、ISP 設備で遮断する措置
  - 同意を得て実施する場合は「フィルタリング」と呼ぶことが多い

- 通信の秘密を侵害する
  - 「アクセスを遮断すること」だけでなく、「アクセス先を監視すること」も通信の秘密の侵害
  - 該当サイトへのアクセスでないものも含めすべてのアクセスが監視されることに注意
    - そのサイトに一切アクセスしない人の通信の秘密まで侵害される

DNS ブロッキング

- ISP のキャッシュDNSサーバで名前解決を失敗させる/虚偽応答を返すことで Web サイトへの接続を遮断する
- 要するに毒入れ



ブロッキングの問題

- 通信の秘密を侵害する
  - どんな目的であれ、形式的には通信の秘密を侵害する
    - ブロッキングしなくても、キャッシュ DNS そのものが通信の秘密を侵害する
    - ルータが通秘を侵害しているのと同じ理屈
  - 違法性阻却事由(刑法35～37条)を満たすか、利用者の同意があればよい
    - ルータやブロッキングしないキャッシュ DNS は正当行為(刑法35条)で違法性阻却
- ブロッキング対象リストを誰が保守するのか
  - 国家権力が保守するのは検閲、表現の自由の侵害になるおそれ
  - 民間で実施するなら中立性・客観性をどのように担保するか
    - オーバーブロッキングの危険
    - 権利者・閲覧者双方から提訴されるリスク

児童ポルノブロッキング

- 緊急避難(刑法37条)により違法性阻却と整理
  - 現在の危難: 今まさにネット上に流通していること
  - 補充性: 児ポ画像の削除や、流通させた者の検挙が容易でない、実効的でないこと
  - 法益権衡: 単に児ポの定義を満たすだけではなく、その中でも特に児童の権利侵害の程度が著しいもの
- 中立性・透明性の高いブロッキングリスト作成
  - インターネットホットラインセンター(IHC)が児ポサイト情報を収集
  - インターネットコンテンツセーフティ協会(ICSA)がブロッキング可否を判断してリスト化

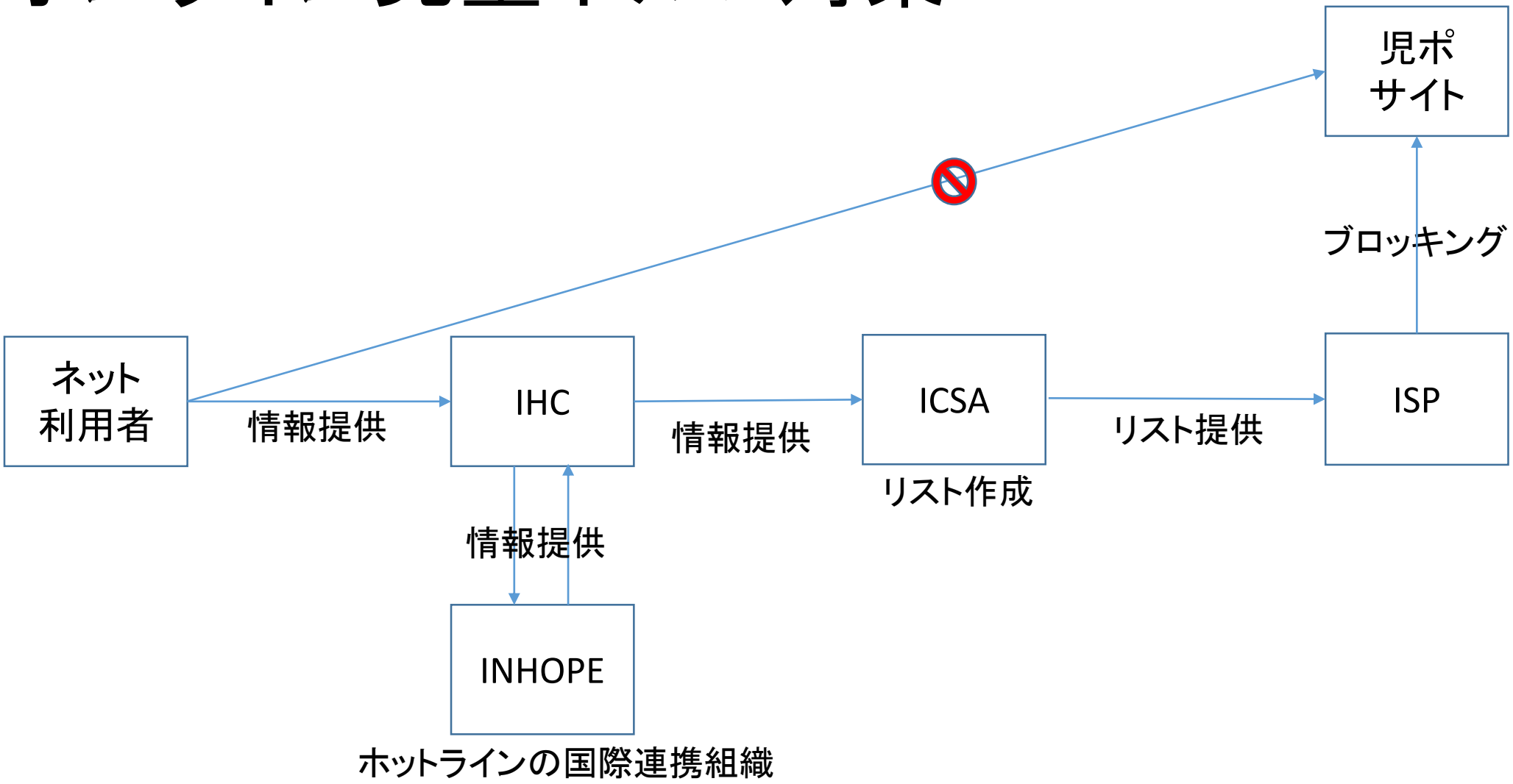
児童ポルノブロッキング経緯

- 2008-2009 警察庁、総務省でネットでの児ポ問題検討
  - 警察庁 総合セキュリティ対策会議
  - 総務省 インターネット上の違法・有害情報への対応に関する検討会
  - いずれも「官がフォローしつつ民間主導で」という方針
- 2009-2011 民間団体(安心ネットづくり促進協議会)で検討
  - 法的整理、技術的課題、ブロッキングリスト運用方針など
- 2011 インターネットコンテンツセーフティ協会(ICSA)設立
  - リスト管理団体
- 2011 各ISPでブロッキング開始

児童ポルノ禁止法

- 1999 児童ポルノ・児童買春禁止法成立
- 2004 児ポ法改正
  - 電気通信回線による児童ポルノの提供及び公然陳列の禁止
- 2005 児童の売買、児童買春及び児童ポルノに関する児童の権利に関する条約の選択議定書批准
- 2012 URL事件 最高裁判決
  - URL(の一部を改変した文字列)を掲示板に書き込み → 公然陳列罪が成立
- 2014 児ポ法改正
  - 単純所持の禁止 (≒ダウンロード違法化)
  - 電気通信事業者に児ポ拡散防止(≒ブロッキング)と捜査協力の努力義務
  - 施行3年後(2018)を目途にブロッキングに必要な措置(努力義務→義務?)

オンライン児童ポルノ対策



マルウェアブロッキング(ACTIVE)

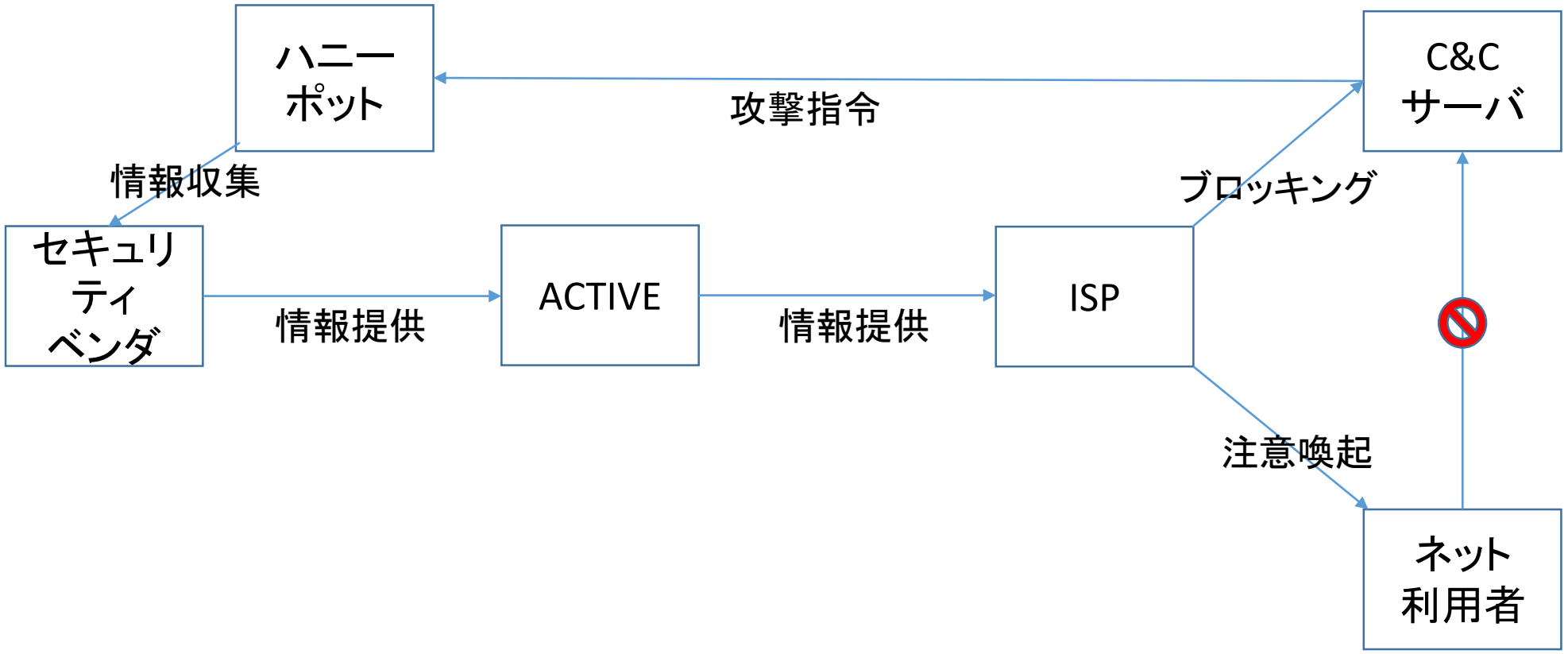
- マルウェアに指令を出す C&C サーバのドメインの名前解決を失敗させることで、マルウェアの被害拡大を防ぐ
- セキュリティベンダ等から提供を受けた C&C サーバの情報を ACTIVE (ICT-ISAC/総務省など)でリスト化

- 契約約款による顧客同意により実施
  - 個別同意ではなく包括同意でよい、と整理された
    - ISP 側はオプトアウトできるようにしておかなければならない
  - 同意によるので、ブロッキングというよりフィルタリングというほうがいい?

マルウェアブロッキング経緯

- 2013 総務省
  - 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会
  - 実証実験 ACTIVE（Advanced Cyber Threats response InitiatiVE）
- 2014 研究会第1次とりまとめ
  - マルウェア感染、DNS amp、SMTP AUTHの認証情報悪用によるspam
- 2015 研究会第2次とりまとめ
  - 他人IDによるPPPoE、脆弱なホームルータ、DNS amp/水責め対策
- 2015 通信5団体 サイバー攻撃ガイドライン第4版
  - マルウェアブロッキング
- 2016 ACTIVE にてマルウェアブロッキング開始

マルウェア感染未然対策



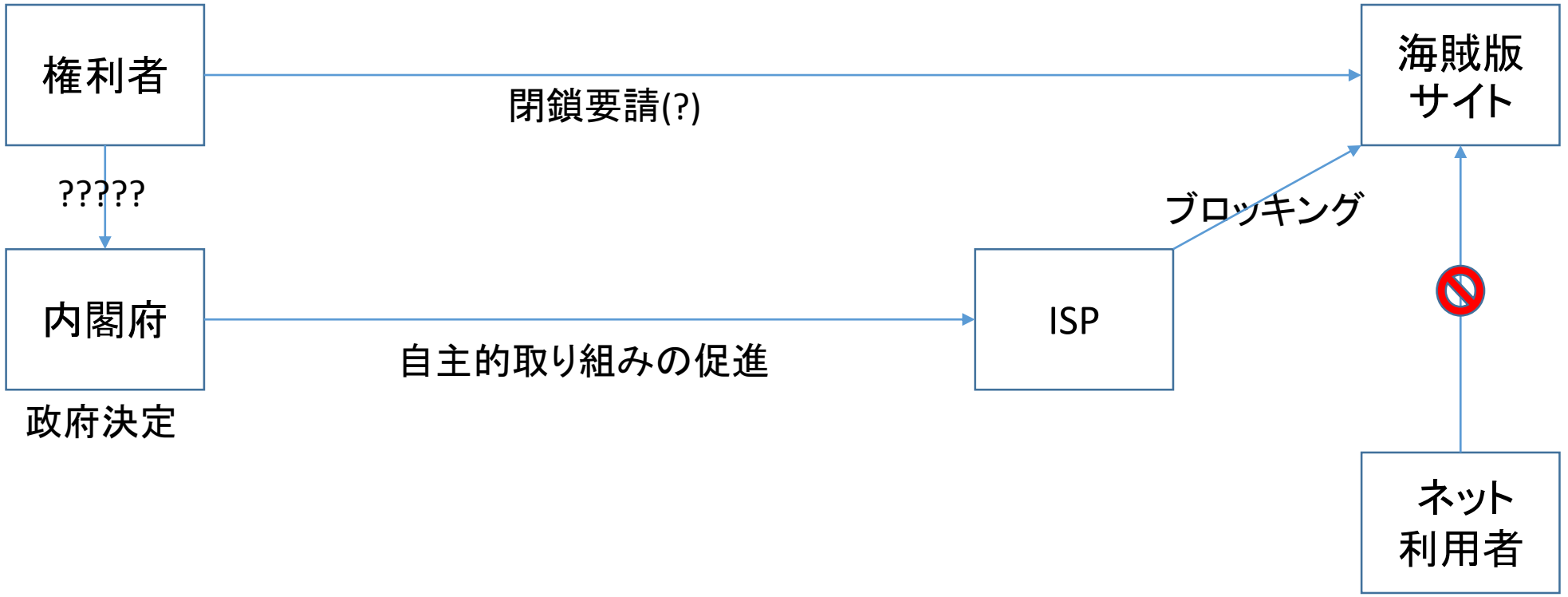
海賊版サイトブロッキング

- 緊急避難(刑法37条)により違法性阻却と整理
  - 現在の危難: 多数のアクセスのある海賊版サイトが現実に存在する
  - 補充性: 削除要請、閉鎖要請、広告出稿停止要請、訴訟等で効果が得られない場合
  - 法益権衡:「財産権であることをもってすなわち回復可能」と断じるのではなく、特に悪質な海賊版サイトに係る状況を勘案した上で、事例に即した具体的な検討が必要
- ブロッキング対象リストの運用があいまい
  - 政府決定で名指しされたサイトは
    - 緊急避難の要件を満たすと明言されていない
    - 名指しされるに至った経緯が不透明
  - 今後のリスト追加削除を誰がやるのか不明

海賊版サイトブロッキング経緯

- 2016-2017 内閣府知財戦略本部の資料にてサイトブロッキングというキーワードが何回か出現
  - が、あまり本格的に議論された形跡は見られない
- 2018/2/16 知財戦略会合で議論
  - 議事録非公開(資料は公開)
- 2018/4/13 知的財産戦略本部・犯罪対策閣僚会議にて決定
  - ISP に自主的な取り組みを促す
- 2018/4/23 NTT グループ ブロッキング実施表明
  - 2018/4/26 NTT com 提訴される
- 2018/6/22 知財戦略本部海賊版対策検討会議第1回

海賊版サイト対策



その他サイトブロッキング

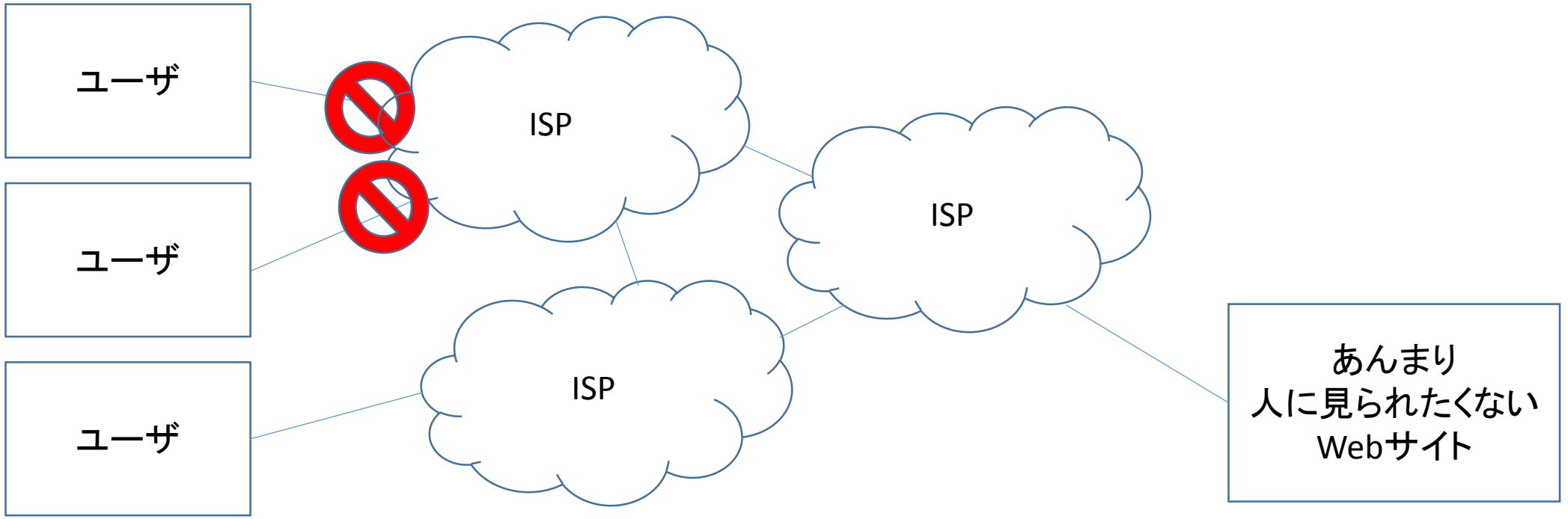
- 通販サイトブロッキング
  - コンビニ無料 Wi-Fi から他社通販サイトをブロッキング
  - 通秘侵害で行政指導(2012)
- 海外では商標権侵害などのブロッキングも実施されている
  - イギリスなど
- イスラム教国ではアルコール宣伝がブロッキング対象になることも
  - マレーシアなど

Inbound/Outbound Port 53 Blocking

- 外部から届く/ 内部から出て行く port 53 宛パケットを一律遮断
- これも通信の秘密を侵害する
- IP53B
  - open resolver なホームルータが DNS amp や水責め攻撃の踏み台にされるのを防ぐ
  - 正当行為(刑法35条)
- OP53B
  - マルウェア感染 PC など外部の DNS を攻撃するを防ぐ
  - DNS ブロッキング回避のために public DNS が利用されるのを防ぐ
  - 技術的には OP25B (正当行為)とほぼ同じだが、法的には別途検討が必要
    - たぶん違法性は阻却できないんじゃないかと…

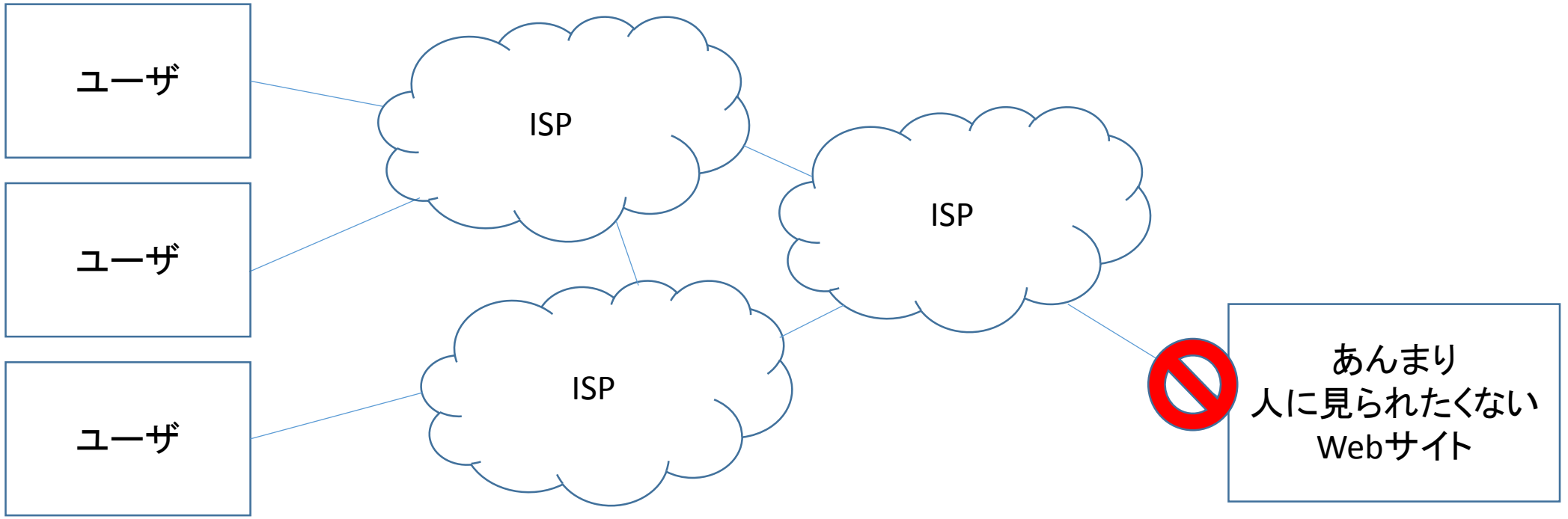
ところで

こうじゃなくて、



ところで

こうあるべきなのでは



よく考えましょう