DNSブロッキング/フィルタリングの法的解釈と実施状況

Internet Week ショーケース in 奈良

2025年7月2日

株式会社インターネットイニシアティブ
ネットワークサービス事業本部 ネットワーク本部 アプリケーションサービス1部 DNS技術1課

其田　学

自己紹介

■名前　其田　学

■所属　株式会社インターネットイニシアティブ

アプリケーションサービス部1部　DNS技術１課

■職務　IIJのお客様向けのDNSサービスの設計・運用など

■DNSとの関わり　前職時に2010年にフルリゾルバーへの署名検証の導入

2011年に権威DNSサービスでのDNSSEC署名の導入など

IIJ JOIN後はIIJのお客様向けのフルリゾルバー、権威DNSサーバの設計、構築など

IIJでのDNSブロッキングの運用

IIJでは、DNSブロッキングとして、児童ポルノブロッキングを実施※1

機能概要

一般社団法人インターネットコンテンツセーフティ協会（以下ICSA）が作成した、DNSブロッキング用のリストを元に、DNSブロッキングを実施

対象サービス

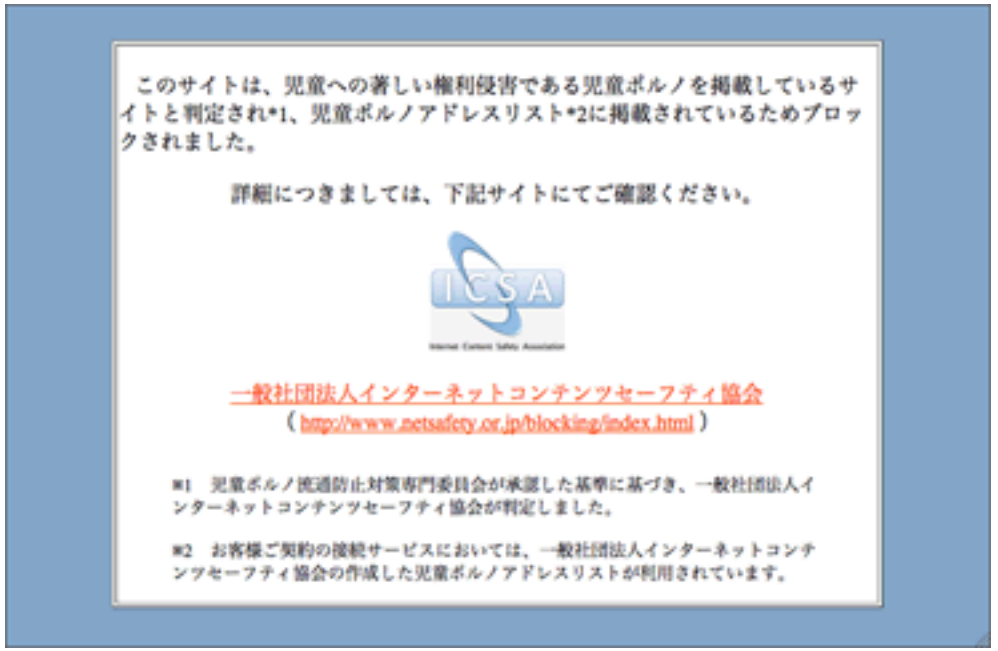
- IIJmioサービス

※1 サービス案内 - 児童ポルノブロッキング対応について https://www.iijmio.jp/guide/blocking/

ブロック時の挙動

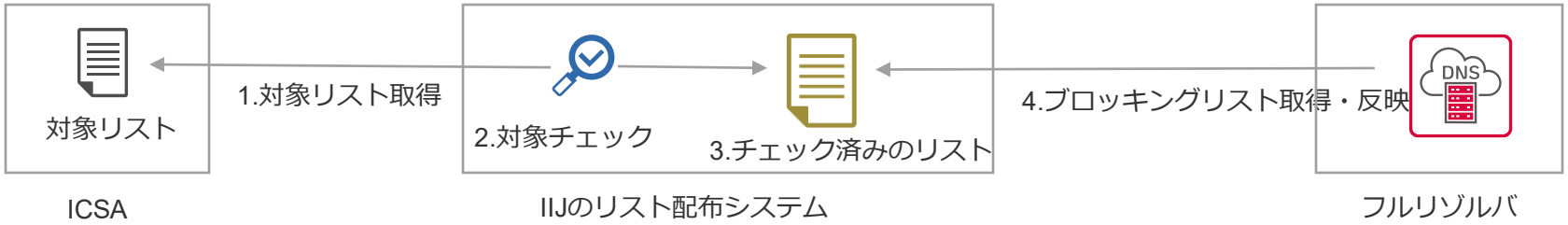
ブロッキング対象サイトにHTTPでアクセスすると、偽のA,AAAAレコードを返してブロック対象になったことを示す専用のWebサイトにアクセスさせます

- いまは常時HTTPS化によって、ほぼ機能してないです。。。



ブロッキング時に表示されるページ（各社共通）

リストの適用方法



1. ICSAから、リストを取得する
2. フォーマットチェック※1、ブラックリストチェック※2、正規化の実施
3. 適用確認用のテスト用のドメイン名※3を追加して、リスト配信サーバに保存
4. フルリゾルバが、リスト配信サーバから対象リストを取得し、適用

ICSAからのブロッキング対象リストの取得から、フリゾルバへの設定反映まで、
全て自動で行われており人間は一切関わらない。

※1 ドメイン名の形式でないものが混入しないかの確認
※2 root-servers.netとか、間違って入ると障害になるものを確認
※3 動作確認時のドメイン名 cpb-test.cns.2iij.net

データの取り扱いで、気をつけていること

- 前述の通り、定常的な運用を人間が関わらないようにする
- 定常運用でログ等に記録されないようにする
  - 自動化プログラムも注意が必要
  - 正常運用時に対象ドメイン名がなるべく出ないように、取得、確認、反映それぞれのフェーズで気を付ける必要がある
- 動作確認は対象ドメイン名以外のものでできるようにしておく
  - 動作確認のために、リストの中身を見たくないため、動作確認用のドメイン名を追加している。
  - 処理が成功したかの監視は、動作確認用のドメイン名が、ブロッキングされている事で確認している
- ブロッキングされたWebページのアクセスログはホスト名やブロッキングされたユーザの特定につながる情報(IPアドレスなど)は記録しない
  - 児ポブロッキングの目的はあくまで児童の権利保護であり、誰がアクセスしようとしたのか調査することではないため

IIJのDNSフィルタリング運用

DNSフィルタリングとして、マルウェアドメイン名フィルタリングを実施※1

機能概要

- IIJが作成したリストを元に、フィルタリングを実施
- 必要に応じて、フィルタされたお客様へ通知を実施
- フルリゾルバのDNSのログを解析して、マルウェアドメイン名の解析を実施

対象サービス

- IIJ接続系サービス
  - IPoEなどを除きほぼすべてのサービス
- IIJ GIO (クラウド)

※1 IIJのセキュリティに関する取り組み https://www.iij.ad.jp/sec-statement/

リストの適用方法は、児童ポルノブロッキングと同じ

- リスト取得部分はことなるが、基本的なチェックや、動作確認用のドメイン名を追加する等は同じ

リスト作成を第３者ではなく、IIJで行うのが大きな違い

- リスト作成とフルリゾルバ運用は社内の別部署
- DNS運用側では、児ポ同様にリストに恣意的な判断を加えず、サーバに反映
- フィルタリングの実施状況について定期的にレポートを公表
  - https://www.iij.ad.jp/sec-statement/

※1 IIJのセキュリティに関する取り組み https://www.iij.ad.jp/sec-statement/

包括同意によるフィルタリング

2019年のフィルタリング開始時は、約款の基づく包括同意にスタート
フィルタリングは原則として個別同意で実施すべきだが、IIJのマルウェアフィルタリングは包括同意で実施

適切な条件を満たせば包括同意であっても有効な同意があるといえるとの解釈がされている

- 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第三次とりまとめ」
  - https://www.soumu.go.jp/main_content/000575399.pdf
- JAIPAほか5団体「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン第6版」
  - https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf

※1 IIJのセキュリティに関する取り組み https://www.iij.ad.jp/sec-statement/

包括同意によるフィルタリング

サイバー攻撃と通信の秘密に関するガイドライン第6版 pp.33-34

a 自身が利用する端末が C&C サーバと通信している場合には当該通信が遮断されるサービスが提供されており、かつこれを希望しない者は検知等の対象にならない。
b 保存された情報が他の用途では利用されず、目的達成後速やかに削除される。
c 照合、記録及び分析を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える。具体的な対応の例については、第二次とりまとめＰ１３参照。
d 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更（設定変更）できるようにする。
e 同意内容の変更の有無にかかわらず、その他の提供条件が同一である契約内容とする。
f 本件対策の内容とともに、照合、記録及び分析を望まない利用者は随時同意内容を変更（設定変更）できること及びその方法につき利用者に相応の周知を図る。具体的には、契約締結時に書面等を用いて明確に説明する他、既契約者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によって周知すること等が考えられる。

（おまけ）ISPのフルリゾルバでのDNSでのフィルタリングの限界

設計者としては、その他提供条件が同一であるというのは負荷が大きい。

仮にカテゴリが増えると、設定が指数関数的に増える(2^n 通り)
ISPで提供しているDNSは、IPアドレスで指定される、指数関数的にIPアドレス利用が増えて破綻する。
- DNSには、HTTPにおけるバーチャルホスト的な機能がないため

下の表はカテゴリ数による設定の数、必要なアドレスの数は大体、設定数1に必要なアドレス数との掛け算
- サーバを共有するか、拠点の数、監視方法等等により変わってきます。

カテゴリ数	設定数
1	2
2	4
3	8
4	16
5	32
10	1024

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ
——IIJはいつもはじまりであり、未来です。