資料９

ブロッキングに関する技術とネットワーク

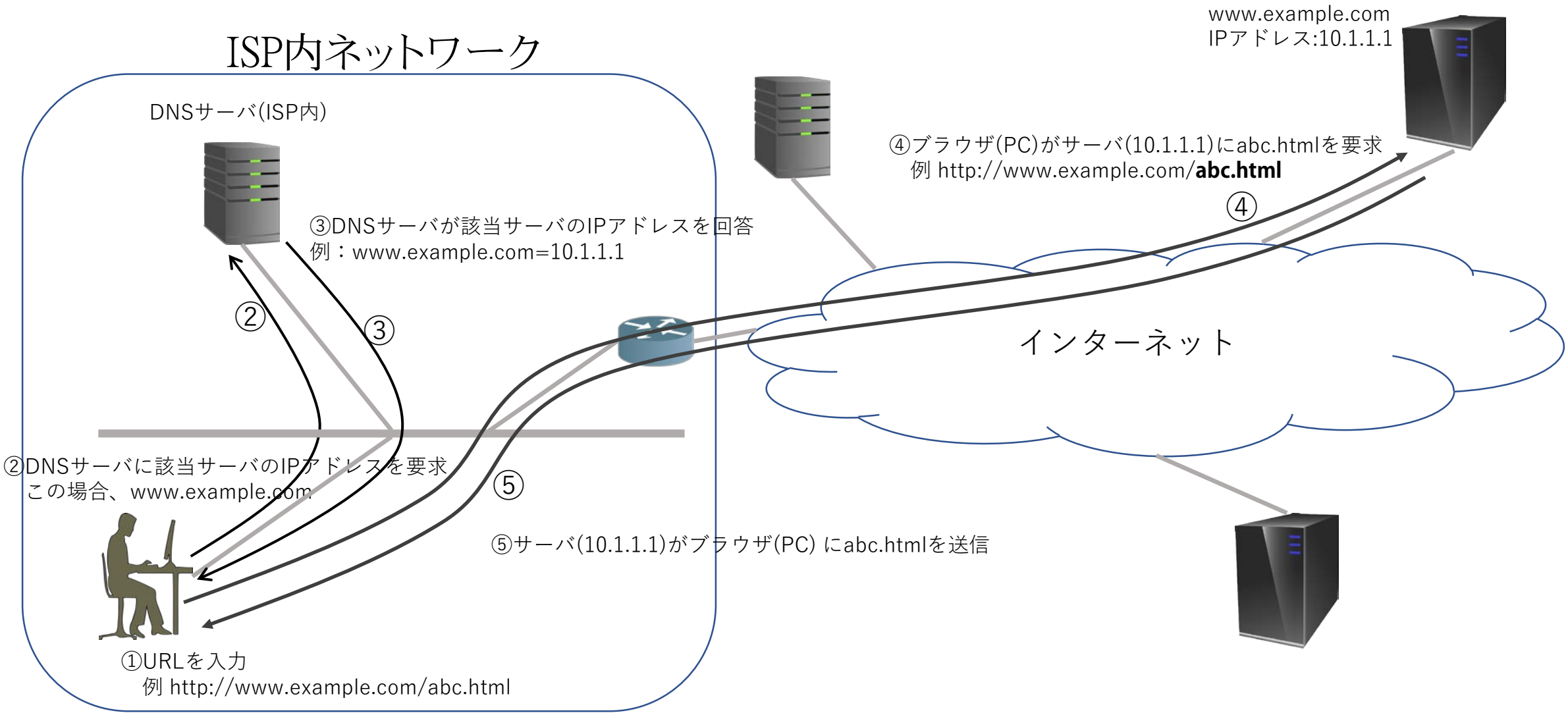
インターネット上の海賊版対策に関する検討会議資料

(一社)日本インターネットプロバイダー協会
副会長兼専務理事
立石　聡明

『ブロッキング』の定義

- ここでいう、ブロッキングはユーザ本人の同意なく特定のサイトを見せない、あるいはポートを利用させないなど、本来インターネット接続サービスで提供される機能の一部あるいは全部を意図的に提供しないこと。
- 青少年保護の為に、親権者の同意を得て18歳以下の子供たちが利用する端末に設定する閲覧防止措置であるフィルタリングとは、本質的に違うものである。

通常のWebサイトへのアクセスとDNSの動き(概要)



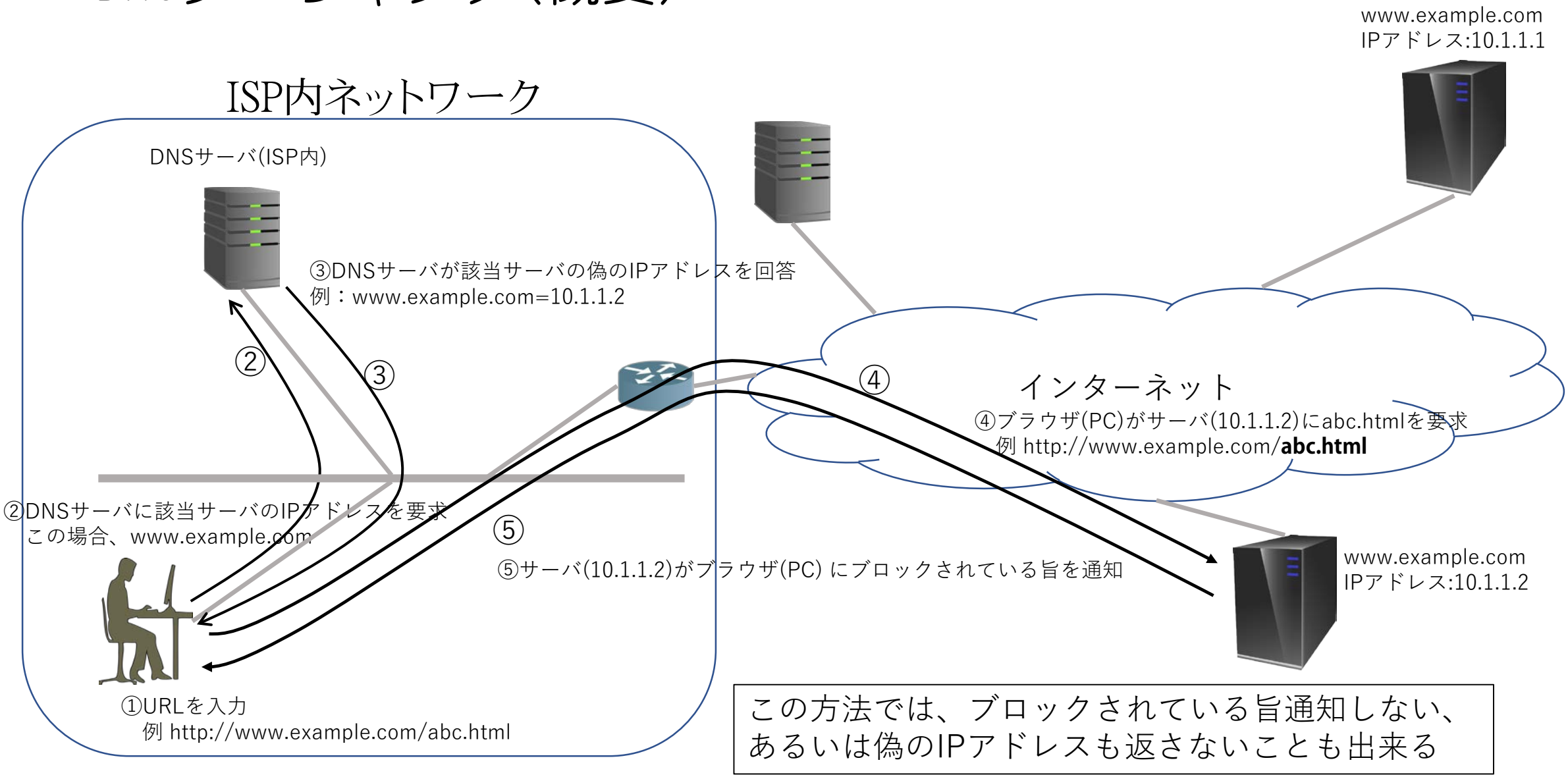
ブロッキングの技術の種類

- DNSブロック
  - Web等閲覧する際、ユーザからリクエストされたWebサイトのIPアドレスとは違う、偽のDNS情報をユーザに返して、該当Webサイトに接続出来なくするもの
- URLブロック
  - 例えば、画像などのファイル単位でブロックすることできめ細やかなブロックが出来る
- ハイブリッド
  - DNSブロックとURLブロックを効率的に使ってファイル単位でブロックする
- IPブロック
  - IPアドレス、あるいはその群単位でブロックする

DNSブロックの概要

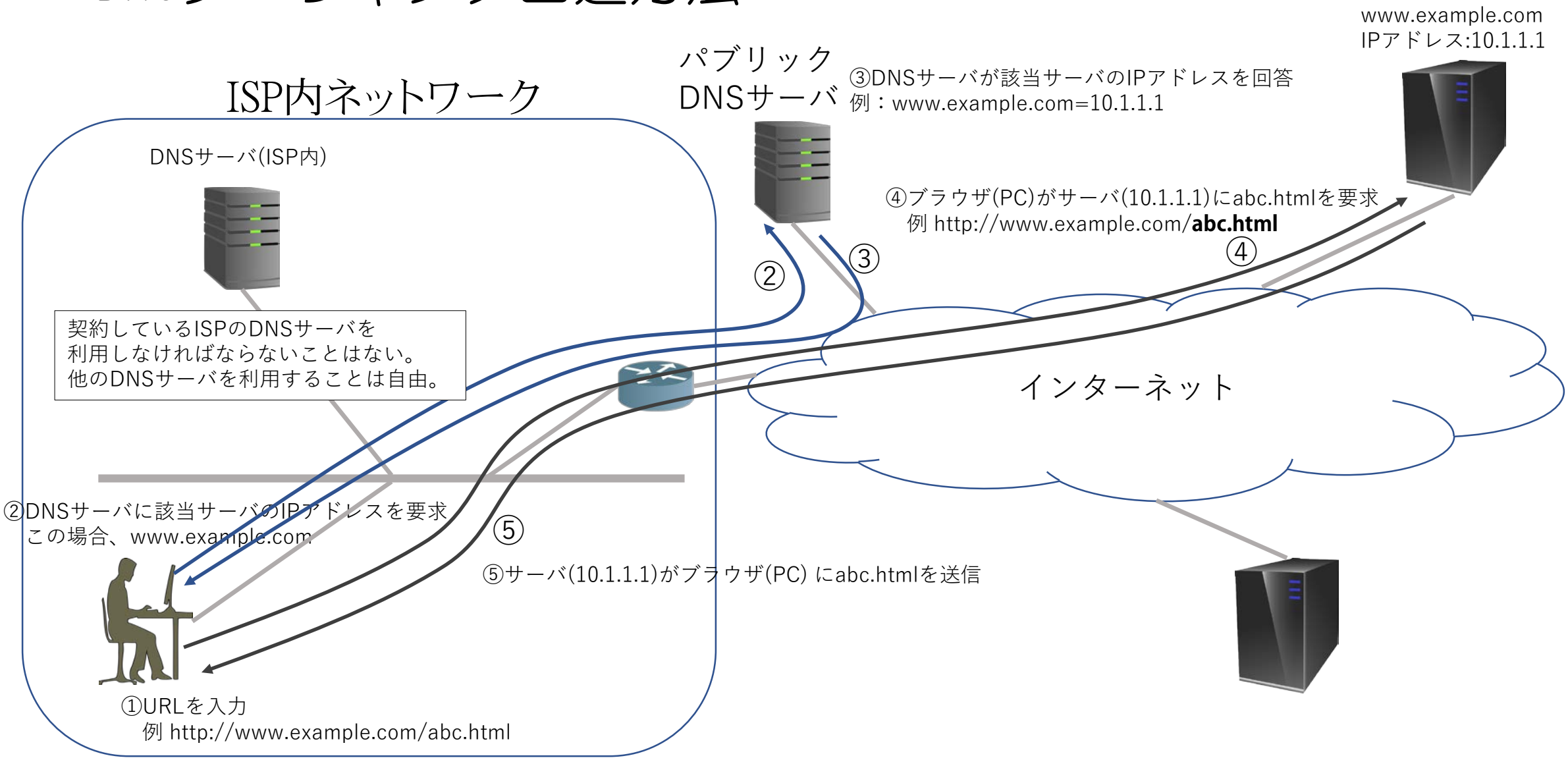
1. DNSブロック
   ユーザがリクエストしたURLのうちサーバ名のIPアドレスをDNSサーバが、偽のIPアドレスを返すことで、接続しようとしたサーバに接続させない方法(別名：DNSポイズニンズ)
2. 回避策
   1. ユーザ側回避策：Public DNSを利用
      1. Google等が公表している、8.8.8.8等に設定するだけで回避
   2. サーバ側回避策：ミラーサイトを多数作ることで簡単に回避できる
      1. 現状では回避策無し
3. ユーザ側回避策への対応
   1. OP53Bで、Public DNSが利用できないようにする。
      1. ISPの指定したDNSサーバのみ使えるようにする
      2. DNSが利用している53番ポートをISPがブロック、迷惑メール対策でやっているOP25BのDNS版
4. 3への回避策：DNS over HTTPS or TLSという技術もツールも既に存在
   1. あるいはVPNでPublic DNSが利用できる所までトンネル化することで、Public DNSが利用可能になる。
5. Google Wi-FiやBuffaloの一部製品などで意識することなく回避できる
   1. CDNが回避する為のツールやアプリを公開している

DNSブロッキング(概要)



この方法では、ブロックされている旨通知しない、
あるいは偽のIPアドレスも返さないことも出来る

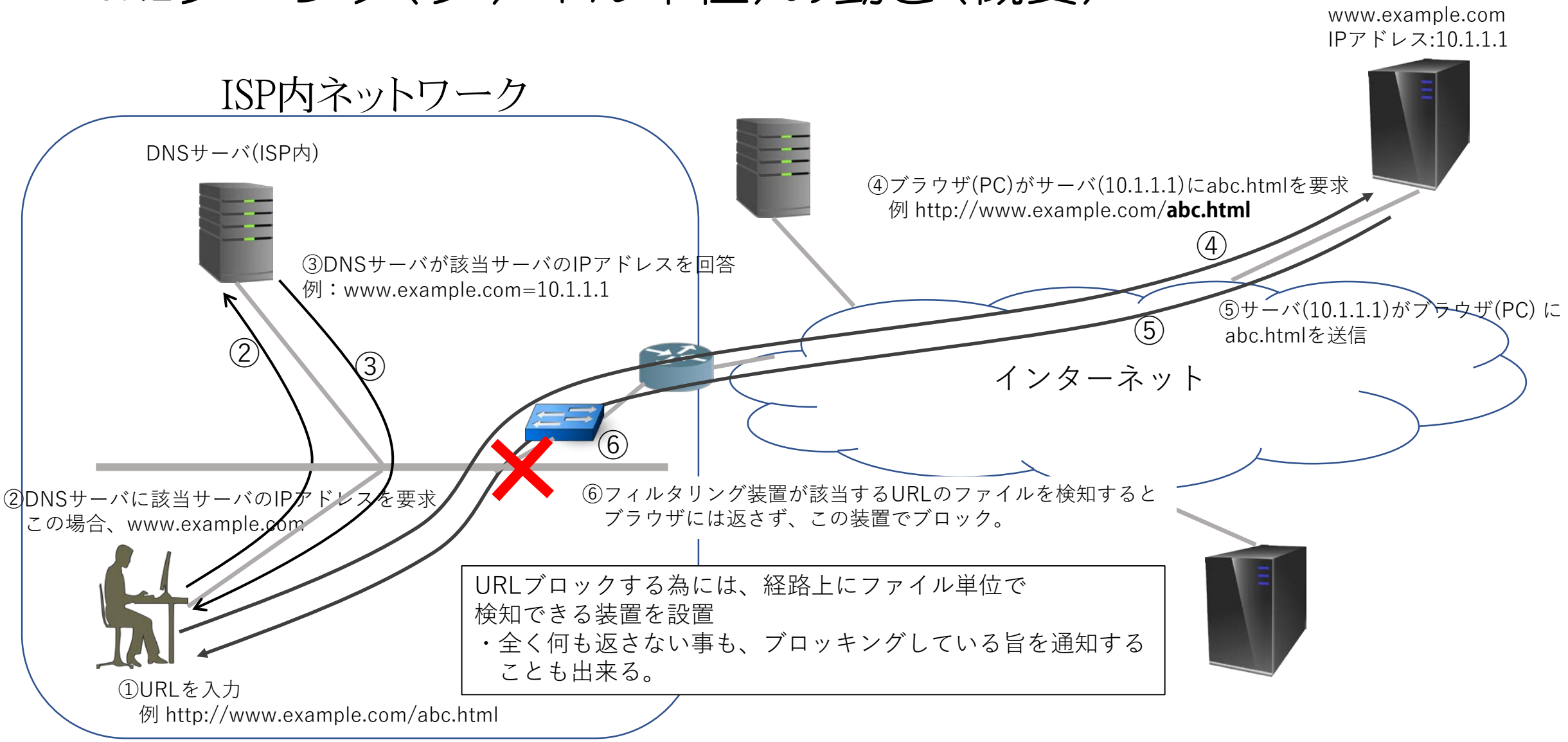
DNSブロッキング回避方法



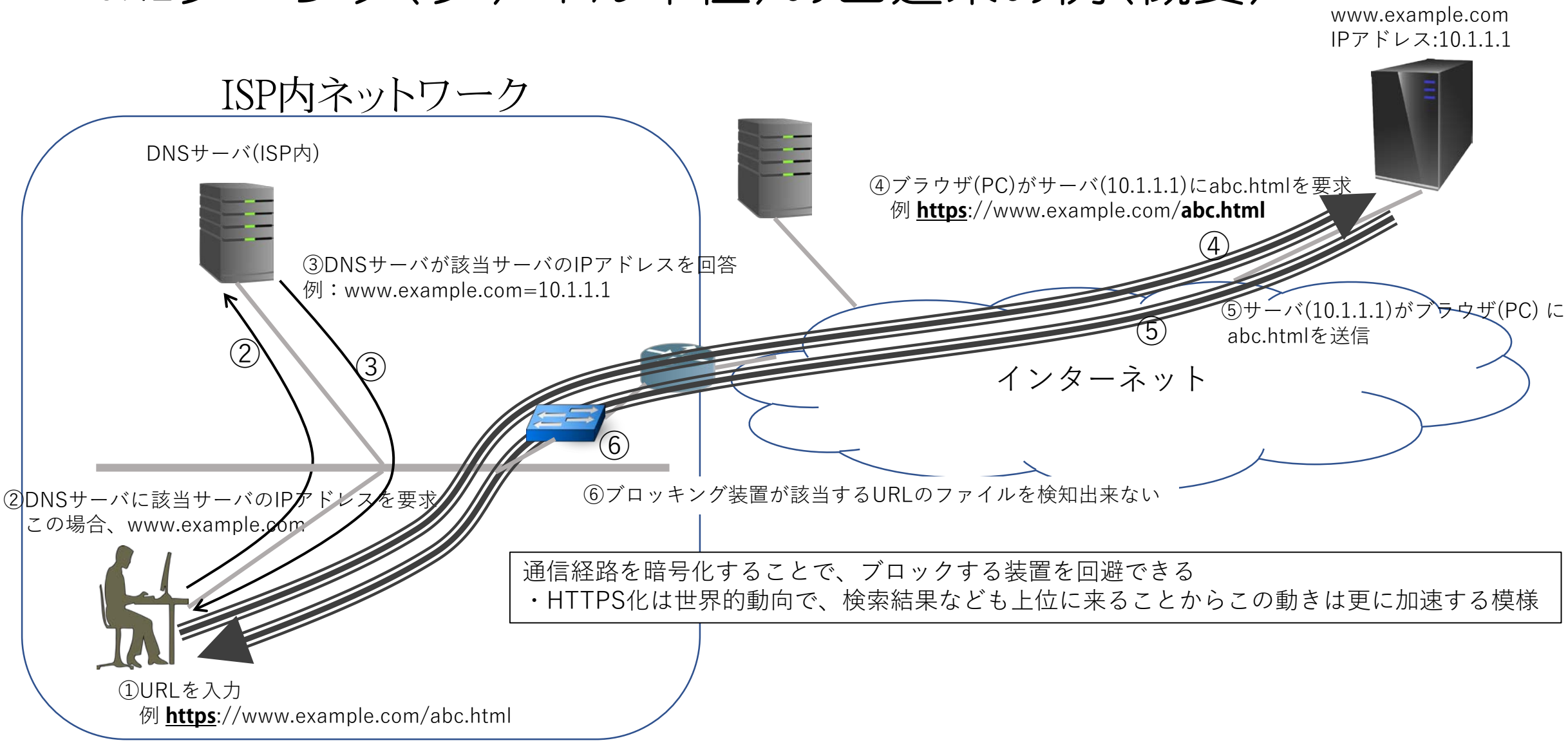
URLブロックの概要

1. URL ブロック：DPI(Deep Packet Inspection) という技術で、特殊な装置をISP内に設置しファイル単位でブロック。
   1. 但し、莫大な費用がかかる。
2. 回避策：サーバをHTTPS化するだけで回避できる
   1. HTTPS化は全世界的な動向であり、検索結果などにも影響する為、更に普及
3. 回避策への対応：一部のサーバに限ってSNI暗号化を復号するする技術があり、HTTPSを平文化することでDPIを利用
   1. ただし、まだ、この技術は確立していない上に、やはり日本全体だと100億単位(？、でも大袈裟ではない)で費用がかかる。
   2. そもそも、これはTLSの脆弱性でもあるため、この穴を塞ぐ技術開発もされている。
4. 3への回避策：HTTPS化する際にSNIを利用しなければよい

URLブロック(ファイル単位)の動き(概要)



URLブロック(ファイル単位)の回避策の例(概要)

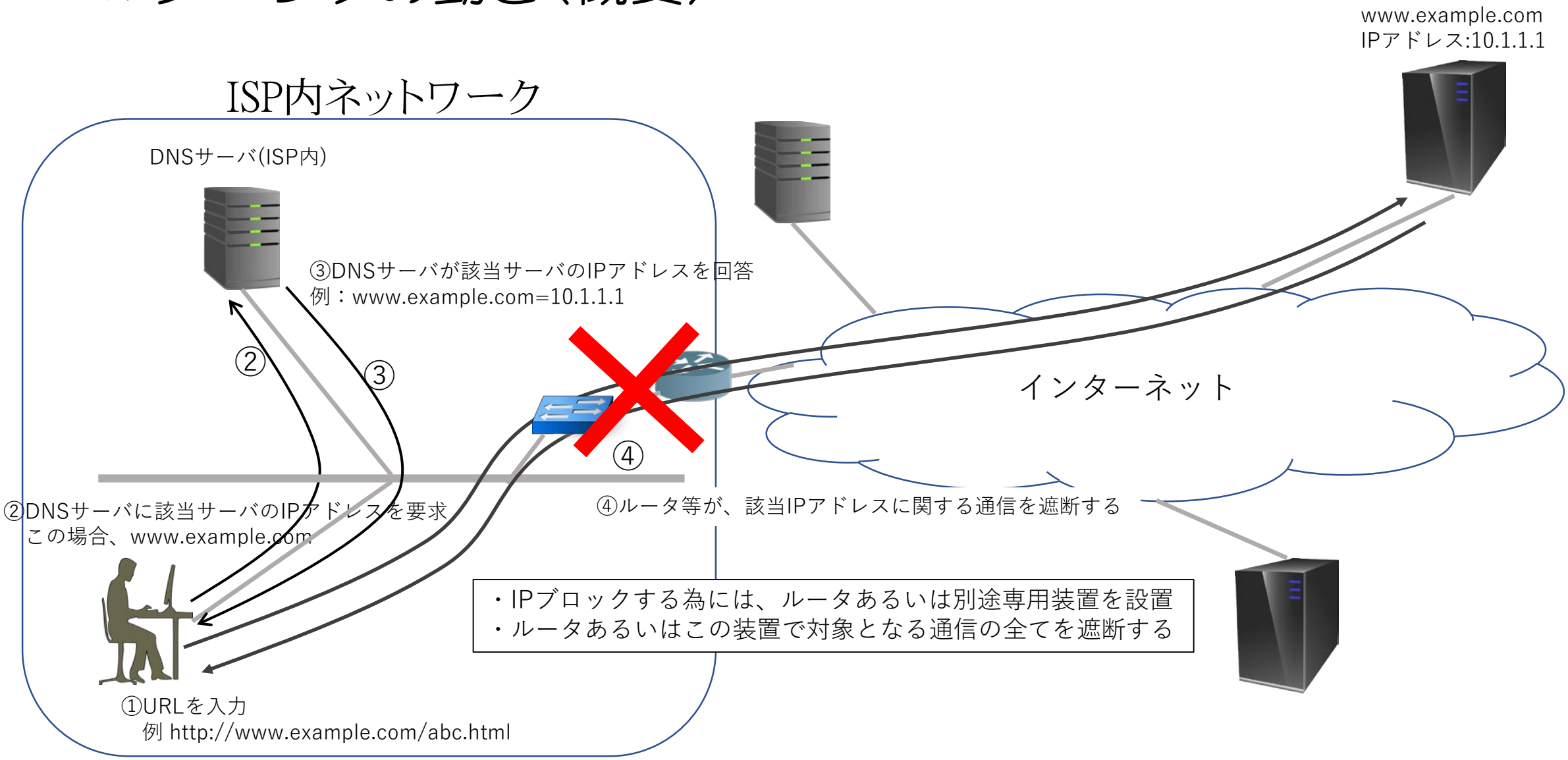


通信経路を暗号化することで、ブロックする装置を回避できる
・HTTPS化は世界的動向で、検索結果なども上位に来ることからこの動きは更に加速する模様

IPブロック

- 該当するサーバのIPアドレスをルータや専用装置で遮断する
- 回避技術は特にない
- 但し、オーバーブロックや他の通信への影響が余りに大きく実際の導入は不可能
  - 1つのIPアドレスに、複数(多い場合は何百ものWebサーバが載っていることはよくあること)のサイトが載っていることが多い為、オーバブロックが発生
  - IPアドレスの割り当ては、割に発生する為、通信障害となる事がある
    - ブロッキングしているIPアドレスがルータなどに割り当て変更されると、そのルータに関係する全ての通信が遮断される
- ジオブロック以外での導入はほぼないと思われる
  - その場合でもサーバ側で行うことが多く、ユーザ周辺のルータで行うことは希である

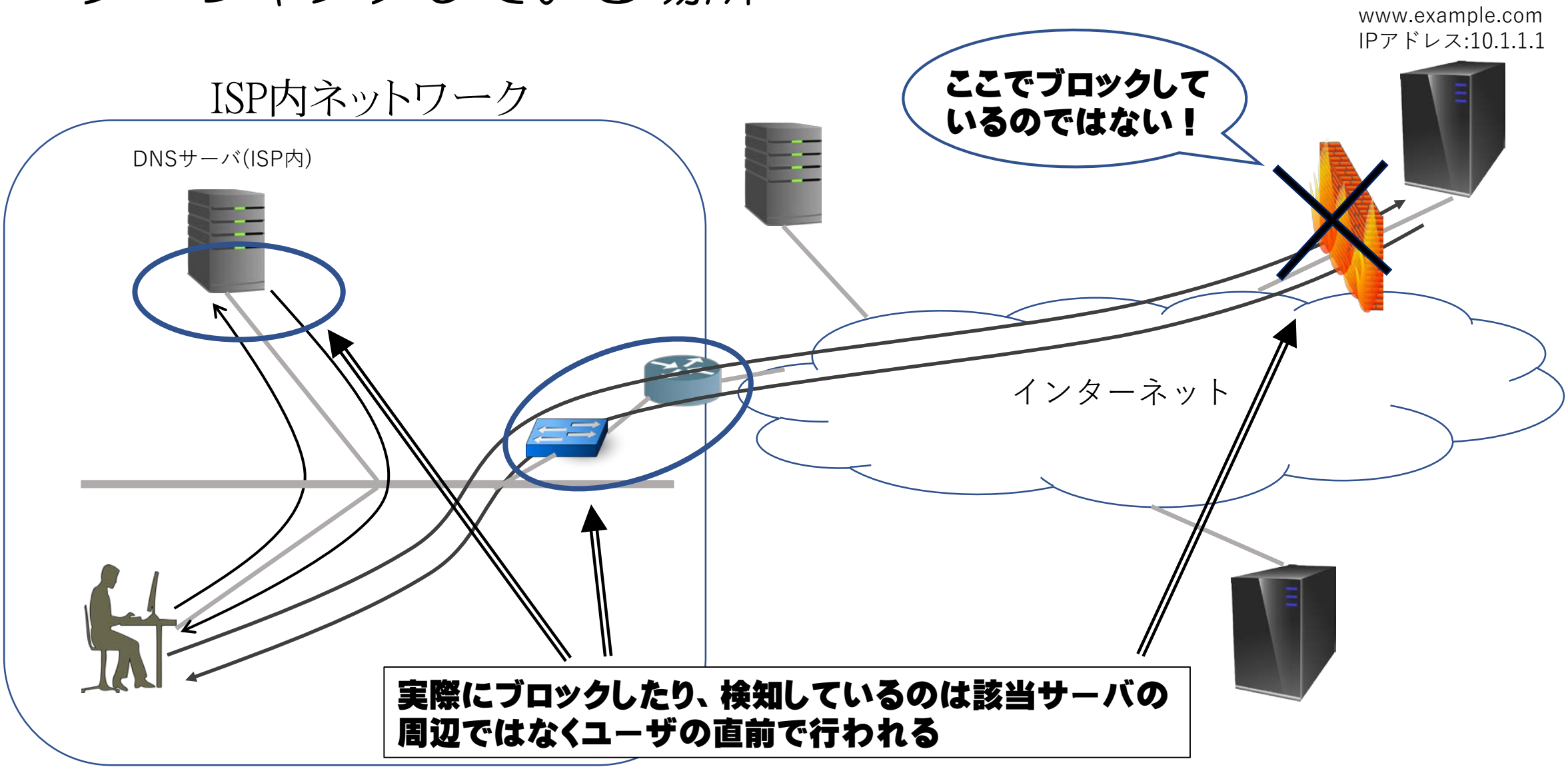
IPブロックの動き(概要)



ブロッキング(通信検知)を行う場所と問題

- ブロッキングというと、接続しようとしているサーバの周辺や国境にある装置で遮断していると思われがちである
- 実際は、ユーザの端末周辺、少なくともユーザが利用しているISPのネットワーク内で行われる
- DNSブロックは、サーバのIPアドレスに対して偽の情報を返す為、単に「遮断」だけでなく「偽情報の通知」という事に対して他の法的に問題が出てこないのかという疑問が残る
  - 通信障害の分析などを行う際、DNSを利用することは通常ある
- DNSブロッキングにしろ、URLブロッキングにしろ、そもそものインターネットの本質をねじ曲げようとしているため、事故が起こる可能性も非常に高く、現にイギリスではたった一枚の画像をブロックするための設定で、Wikipedia全体が見えなくなってしまうと言う事故も起きている。

ブロッキングしている場所

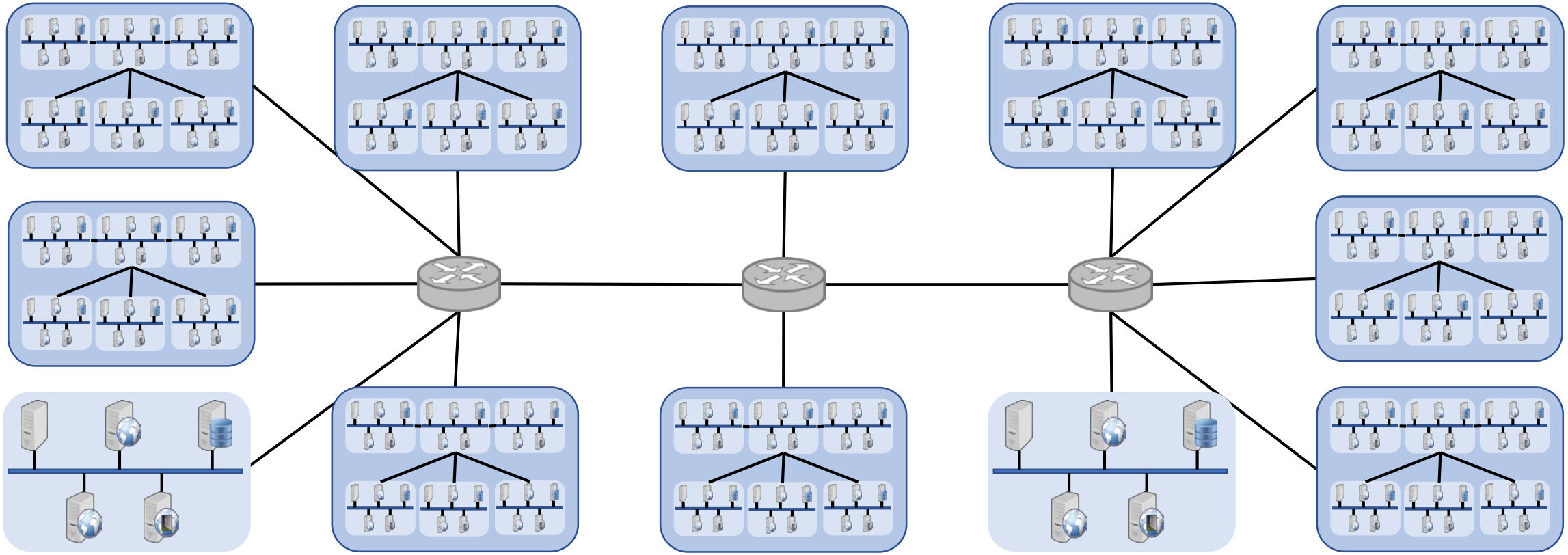


CDNの機能とその概要

- CDN(コンテンツデリバリーネットワーク)は、対象サーバからユーザの端末へいち早くデータを届ける為のネットワーク
- インターネットを利用する際必要なIPアドレス
  その数は、IPv4で約43億個、IPv6で340澗個ある
  - IPv4アドレスはその割り振りが既に終了
  - 340澗個は340兆の1兆倍の1兆倍
  - これらの端末を接続する為のネットワークは非常に複雑
- 日本のネットワークだけでもその全貌を正確に把握することは非常に困難
- ネットワーク的に遠いサーバへ早くデータを届ける為には、別途、高速道路とも言えるバイパス・ネットワークが必要
- このネットワークするには、情報提供者が利用料を払う必要がある

一般的なネットワークイメージ図

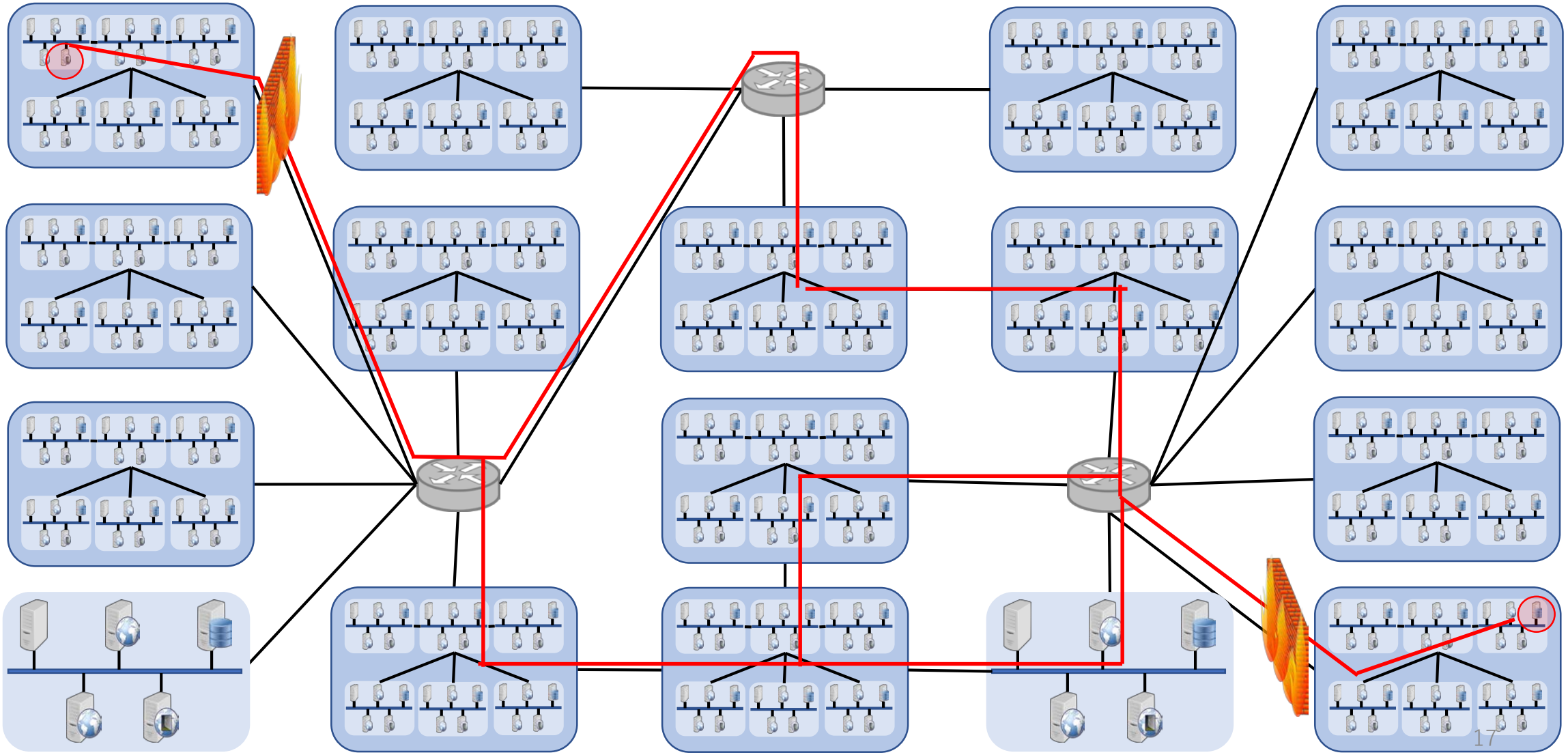
イメージ図



実際にはこの数億倍(?)複雑なネットワーク

- 端末間の通信経路は複数ある
- ブロッキングするためには，どちらかの端末の直近で行う必要がある

イメージ図



CDNはこの複雑なネットワークをバイパス

イメージ図