RITSUMEIKAN

# 技術に詳しくない方でも分かる？！
# ブロッキングの技術的課題

立命館大学情報理工学部
上原哲太郎

# そもそもHTTPというのはどういうものか

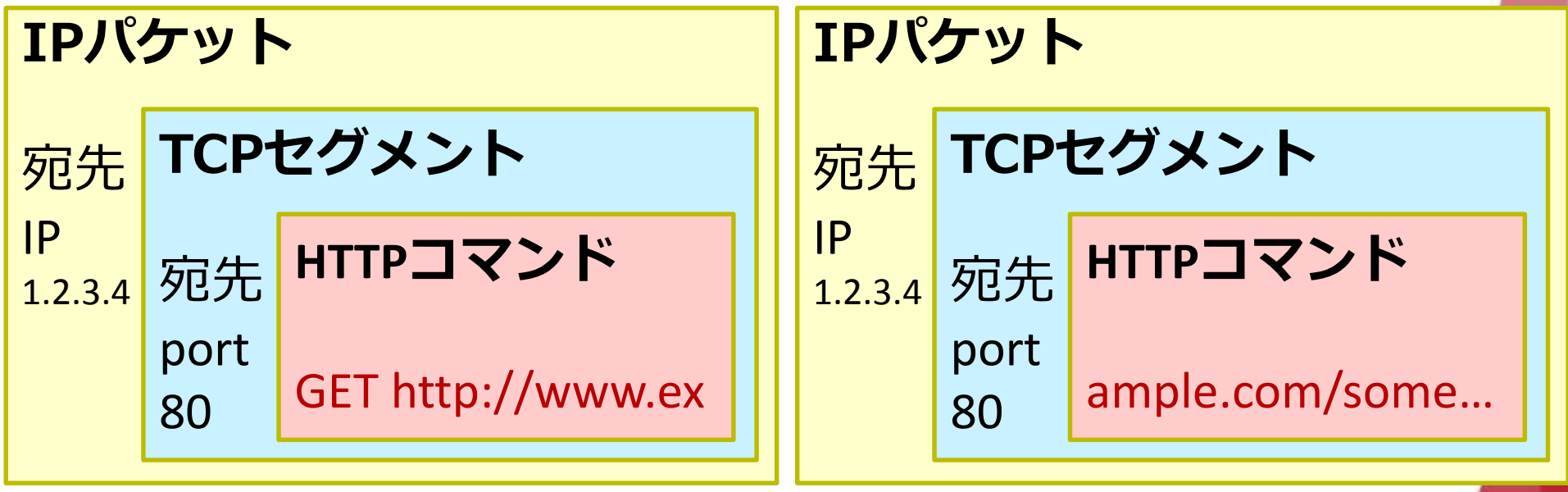
http://www.example.com/somewhere/file.html

ホスト名　　ファイルパス名

- Webブラウザがこれを受け取ると…
  - DNSを使ってホスト名からWebサーバのIPアドレスを得る
  - そのIPアドレスに向けて TCP port 80でTCP接続
  - そのTCP接続を用いてHTTP GETプロトコルでURLをWebサーバに伝え，ファイルを取得
  - そのファイルがHTMLである場合には，埋め込まれた画像等についても同様にURLに従いHTTPでファイルを取得
  - それを組み立てて（レンダリング）Webページを表示
- Proxyがある場合にはブラウザはURLをProxyに投げ，ファイル取得手続きの代行を依頼
- httpsの場合にはTCP portが443になり，TCP接続は暗号化
- このどこかを妨害すればブロッキングが成立

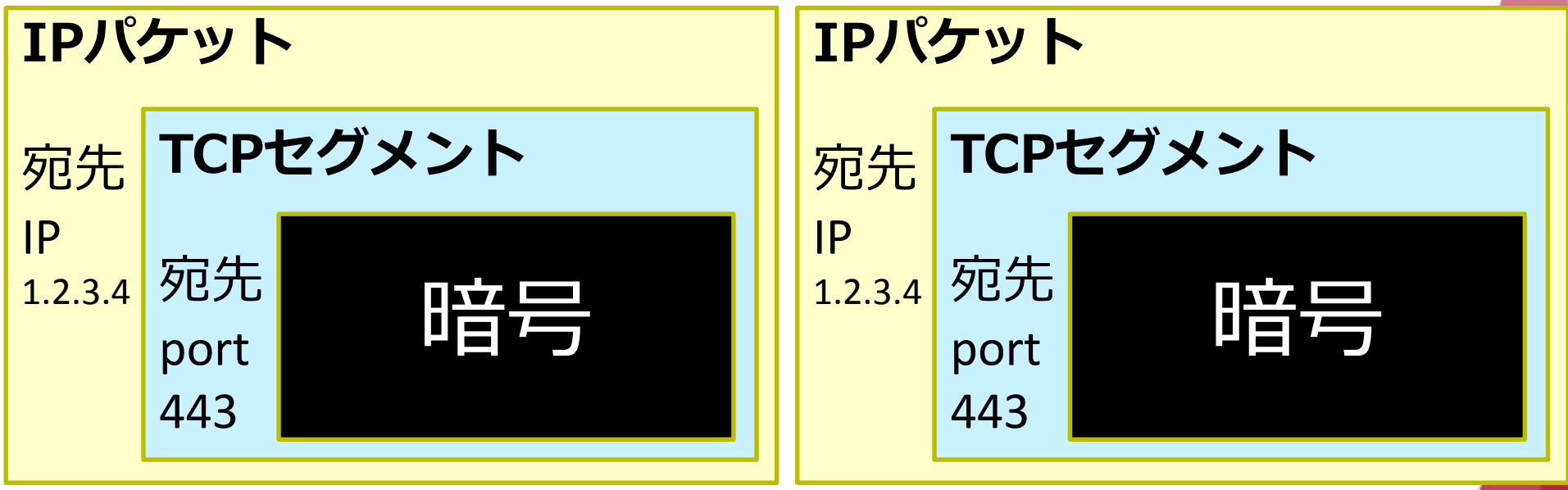
WebサーバのIPアドレスは分かる
URLは暗号化され分からない

# HTTPリクエストを含むパケットのイメージ



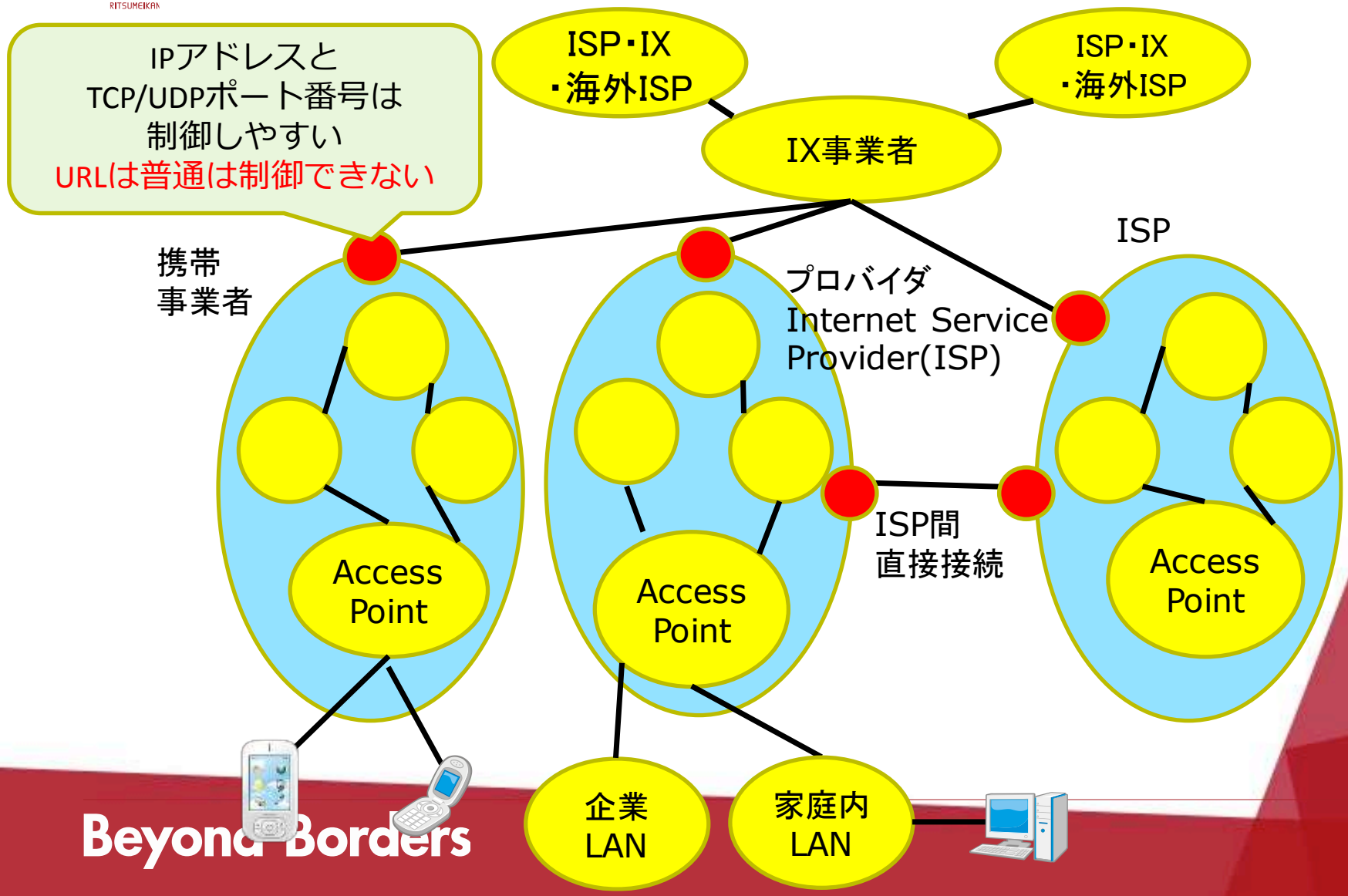

- IPパケット・TCPセグメントはIPパケット単位で制御可
- HTTPは複数のIPパケットを集めないと中身がわからない
  - この仕事は通常ISPが運用している機器では出来ない（要DPI機器）
  - 技術的困難→運用コストがバカ高い　費用負担どうするの？？

# HTTPSリクエストを含むパケットのイメージ




- IPパケット・TCPセグメントはIPパケット単位で制御可
- **TCPセグメントのヘッダより内側は解読不能**
  - なのでHTTPSを含む場合はURLによる制御はできない

# ISPはIPアドレスとポート番号は制御できるがURLは普通は制御できない！



# ところでDNSはどうなってるのか

- DNSサーバ（resolver）は
  通常ISPがそれぞれ所有しており
  管理下にある
  - 通常，各端末は自動設定により
    接続ISPのDNSを利用する
- なので
  「特定のホスト名に対して
  ウソのIPアドレスを返す」
  というDNSサーバを立てるのは比較的容易
  ∴DNSによるブロッキングが
  ISPにとっては比較的コスト低
  URLのうちホスト部だけなら制御可能

設定すればISP外の
DNSサーバ利用可能
（Public DNSなど）

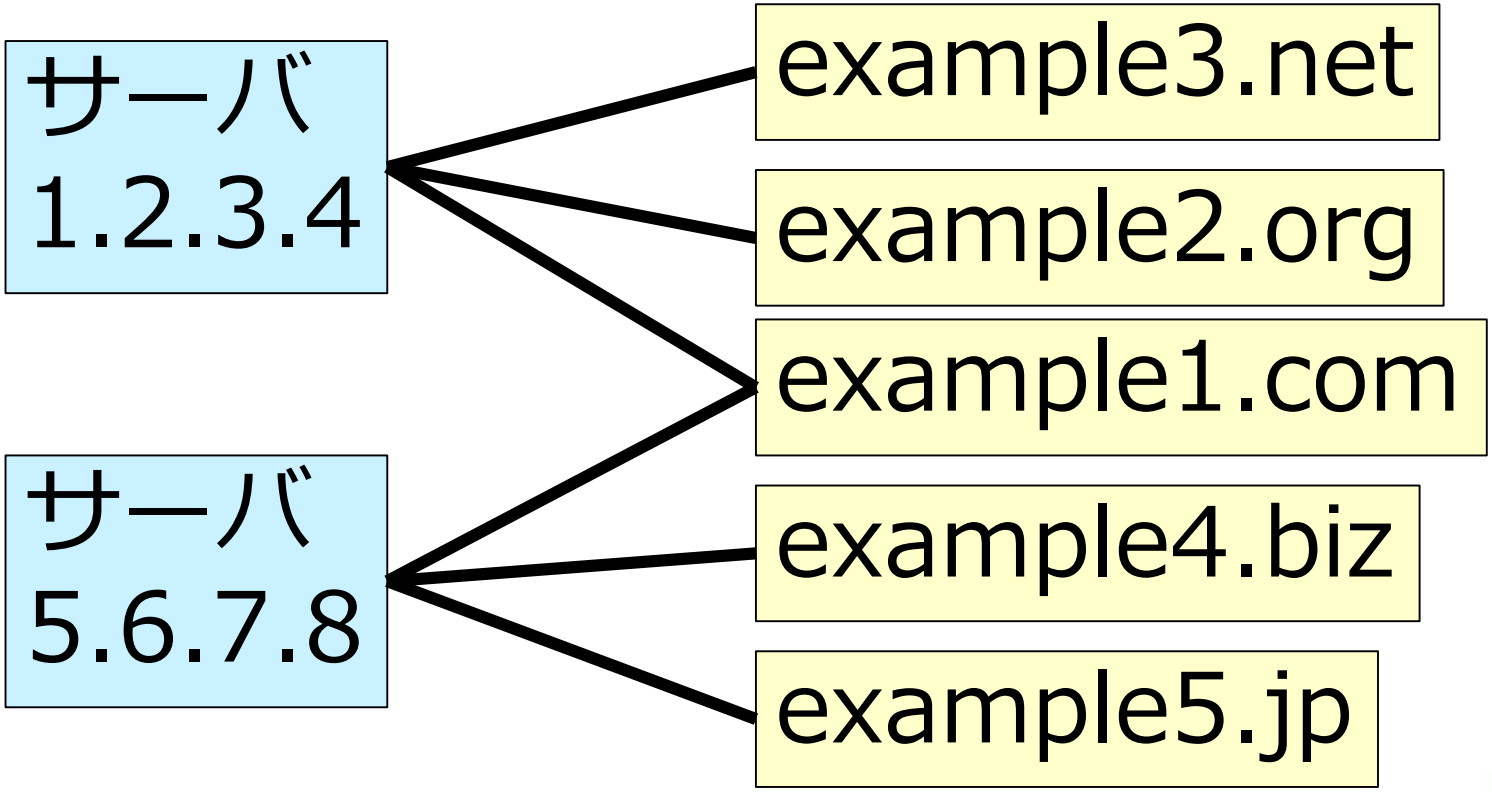
# 余談：ISPがブロッキングを目的として自DNSの利用を強制することは可能か？

- 技術的には「今なら」可能
  - DNS over HTTPSが普及するまで限定の話（Androidが標準装備する予定で急速に普及しそう）
- 具体的にはOP53Bという技術
  - SPAM対策のOP25Bで実績はある
- ただし制度的には相当困難と思われる

# サーバのIPアドレスで止められる？

- IPアドレスとWebサーバホスト名は**一対一対応でない**
  - Virtual Hostingにより多数のHost名が1つのサーバに
  - 1つのホスト名に負荷分散を目的として多数のIPアドレスを付けることがある
    - それを大規模に請け負うのがConent Devilery Network (CDN)
- よってホスト名やIPアドレスで止める場合は**オーバーブロッキング**や**漏れ**が起きえる

# ホスト名とIPアドレスの複雑なカンケイ



# オーバーブロッキング問題・ブロッキング漏れ問題

http://www.example.com/pirates/*
を止めるために
www.example.com　をDNSで止めると…
http://www.example.com/honest/*
も止まってしまう（というか全部止まる）
IPアドレスベースで止める場合には
www.example.comのIPアドレスが
1.2.3.4, 5.6.7.8 等多数になれば
全部止めるのは大変で漏れが出る
（しかもどんどん増えるかも・変えるかも）
IPアドレス1.2.3.4を止めれば
www.example2.net www.example3.orgも止まる

比較的運用コストの低いはずのIPアドレス/ホスト名ブロッキングも実運用は簡単ではない

# URLベースのブロッキングは本当に大変

- http://www.example.com/pirates/と
  http://www.example.com/honest/ を
  区別にするにはURLベースブロッキングが必要
- そもそもIPパケットを複数集めて
  HTTPメッセージを組み立ててから
  通すか止めるか考える必要
  - Deep Packet Inspection (DPI)
- 特別な機器が必要な上大変処理が重く
  現在の高速なインターネットでは
  技術的に困難で運用負荷が高い
  実現しても高価な機器が多数必要