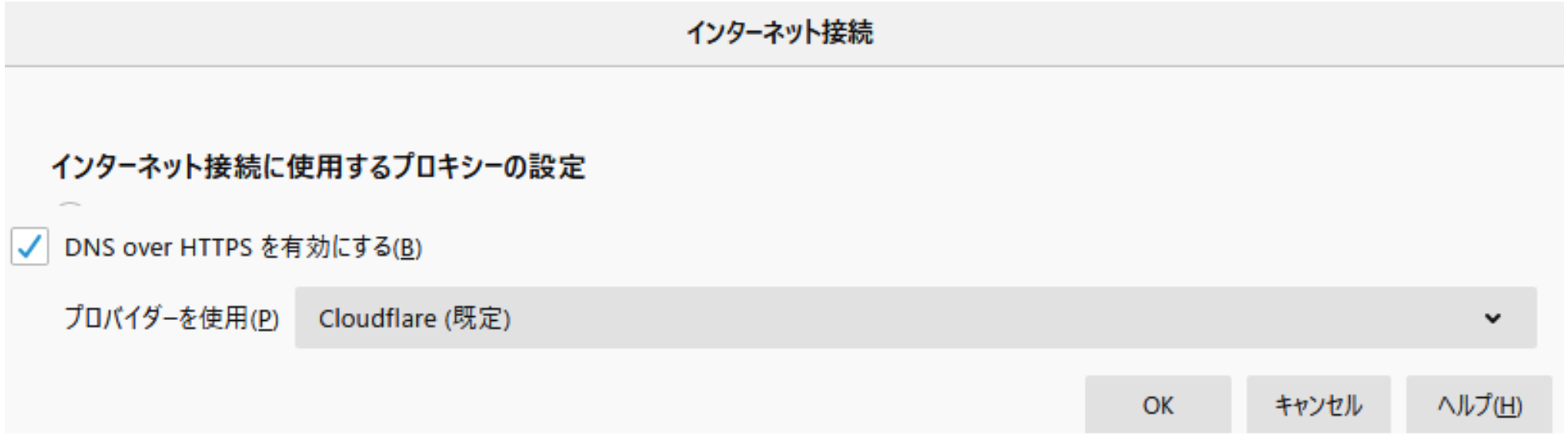
DNS over TLS/HTTPS over CGN

Kazunori Fujiwara
fujiwara@jprs.co.jp

FirefoxでのDNS over HTTPS設定

- Firefoxで、設定→接続設定 を開く
- インターネット接続の画面がでる
- 一番下に「DNS over HTTPSを有効にする」というチェックボックス
  - チェックすると名前解決にDNS over HTTPSを使用
  - 将来のリリースでは標準で有効に
- 規定値は Cloudflare

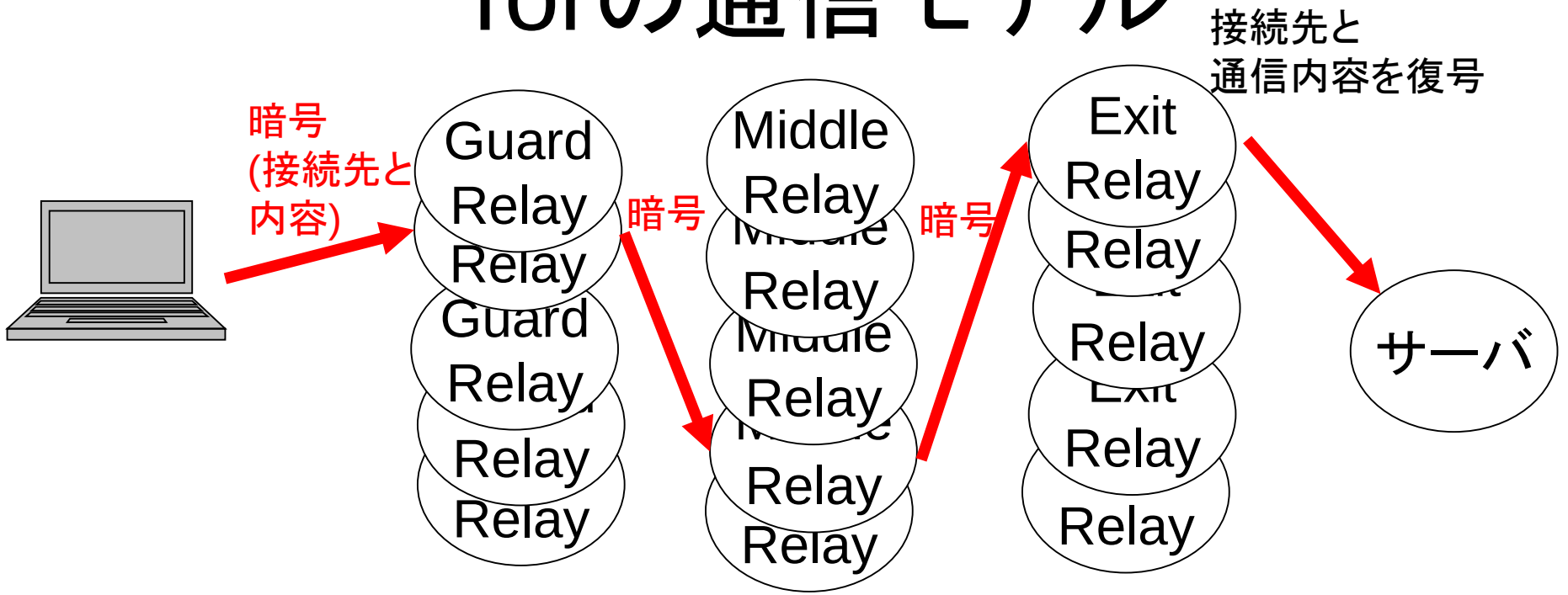


DNS over HTTPS/TLS の問題

- DoH, DoTプロバイダは中身と送信元IPアドレスを知る
  - TLSを終端して中身をみて名前解決
  - 接続元IPアドレスも当然知っている
- DoH, DoTプロバイダのプライバシーポリシー依存
  - Google, Cloudflare は電気通信事業法で縛られない
  - 中身を見ないと言っているが、、、

- 送信元IPアドレスだけでも、隠したい

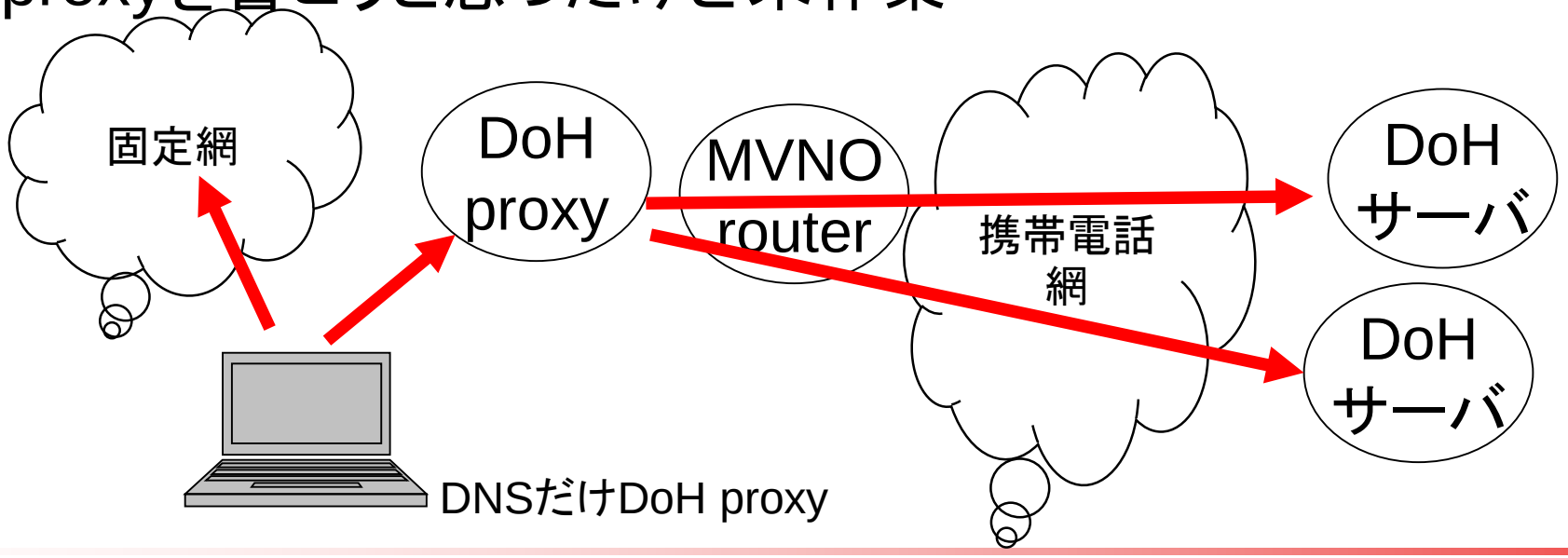
Torの通信モデル



- Guard Relayは送信元を知るが、中身と接続先を知らない
- Middle relayは送信元と中身と接続先を知らない
- Exit relayは接続先と中身を知るが送信元を知らない
- これを一台でできないか？

DNS over TLS/HTTPS over CGN

- 森(NAT)の中から通信すれば送信元はわからない (どこの森かはわかる)
- IPv4アドレスは枯渇していてMVNOの多くは100.64.0.0/10 ISP Shared Addressを使用
- 複数のDoHプロバイダを使いまわす (qnameの一部でハッシュ?)
- DoHのTCP接続を、不定期に切断して張り直し (CGNポート番号変更)
- というproxyを書こうと思ったけど未作業



開示請求

- CGNの変換履歴は記録され、弁護士による開示請求でIPアドレス、契約者まで特定される可能性あり
- 悪意ある行為がなければ開示請求されない
  - 見るだけ、DoH/DoTだけなら開示請求されない
- Webサーバではポート番号を保存していないことがある
  - 一つのIPアドレスを複数ユーザで共有するCGN配下なら開示請求されても問題ない？
  - 共有されたユーザすべてを捜査して逮捕されている事例あり
    - 悪用しなければよい

緩いDNS over HTTPS over CGN

- IPv6をdisable (あるいはv6非対応MVNO)
  - IPv6 privacy address？
  - これではIPv6普及反対派認定されてしまう問題
- CGN配下の100.64.0.0/10のアドレスであることを確認
- FirefoxでDoH有効
- 情報を抜かれるプラグイン類・Cookieなどoff
- これで悪さをしなければ、CGN配下ではないときより、プライバシーはましか？
  - 時系列のクエリ名一式と、CloudflareまたはGoogleへのアクセスを対応づけて分析はされそうだけど
  - ランダムなタイミングでDoH connectionを切断する必要はありそう