Infoblox
CONTROL YOUR NETWORK

DNSのプライバシー対応とその影響

神明達哉

2015年10月23日

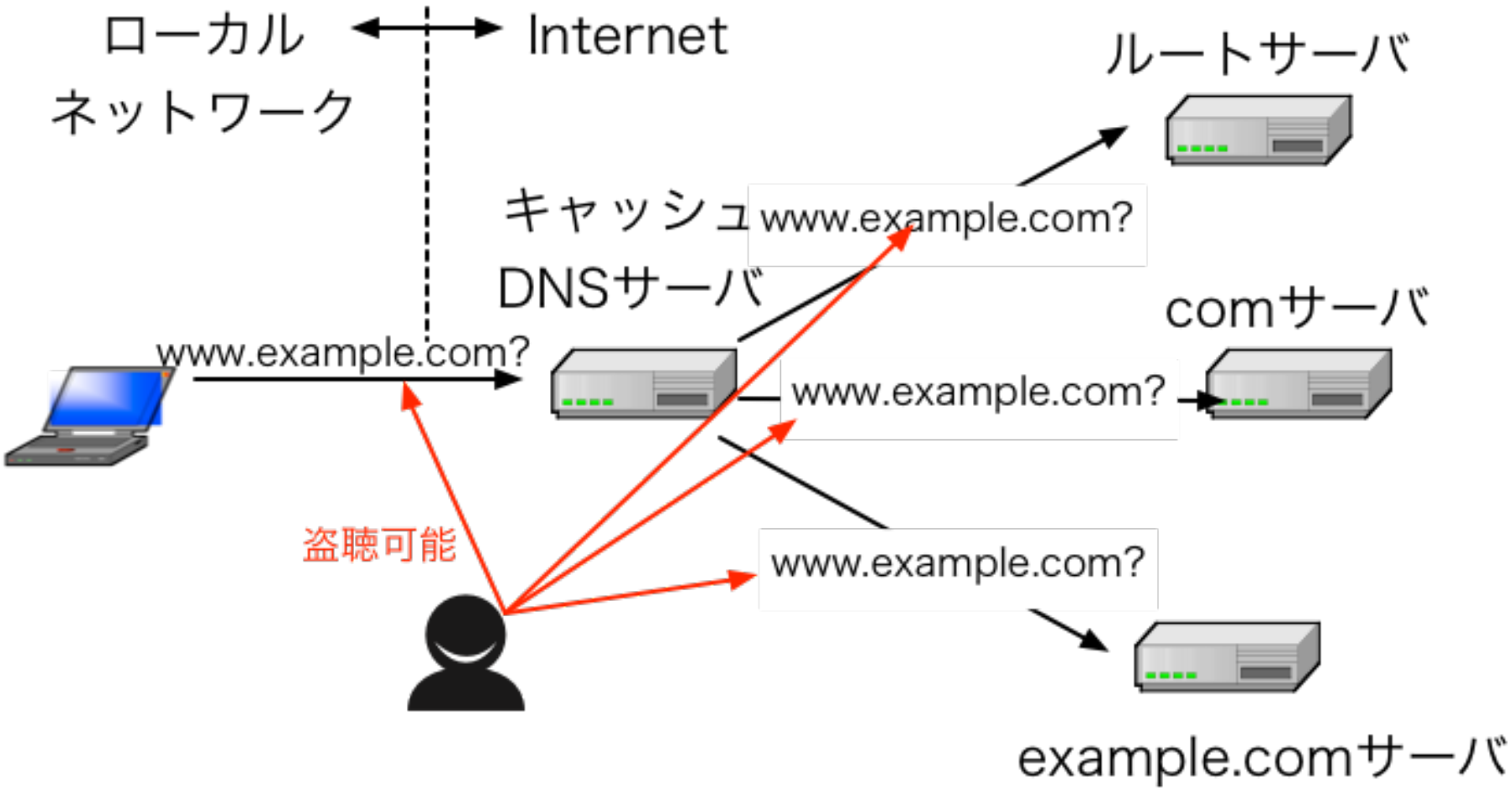
DNSとプライバシー

- 公開が原則のプロトコル
  - ゾーンのデータへのアクセスは原則として制限なし
  - サーバ・クライアント間の暗号化なし
- …が、IETF全体のプライバシー強化がDNSにも波及
  - 米NSAによる盗聴騒動でのプライバシー意識の高まり
  - 2013年11月IETFプレナリで全体セッション
  - 2014年10月“dprive” IETF wgの立ち上げ
  - 2015年8月Problem statement RFC発行(RFC7626)
  - クエリ短縮化(query minimization)の文書化→近々RFC?
  - DNS/TLSを暗号化プロトコルとして採択→WGLC中
  - 2015年10月 DNS/TLS用TCP(とUDP)ポート853が仮割当て

DNSによるプライバシーリスク

- クエリ名
  - 特定のサービス利用を開示: some.badsite.example
  - 特定のアプリケーション利用を開示: SRVレコード
- 送信元IPアドレス
  - ユーザを特定する情報
  - 通常スタブ-キャッシュ間のみだが、client-subnet EDNSオプションによる例外あり
- DNS特有の事情
  - 通信はすべて平文
  - 様々な「盗聴」ポイント
- 「どの程度深刻なリスクか」には議論の余地あり
  - 気にする人は必ずいるし、過度の楽観視も危険

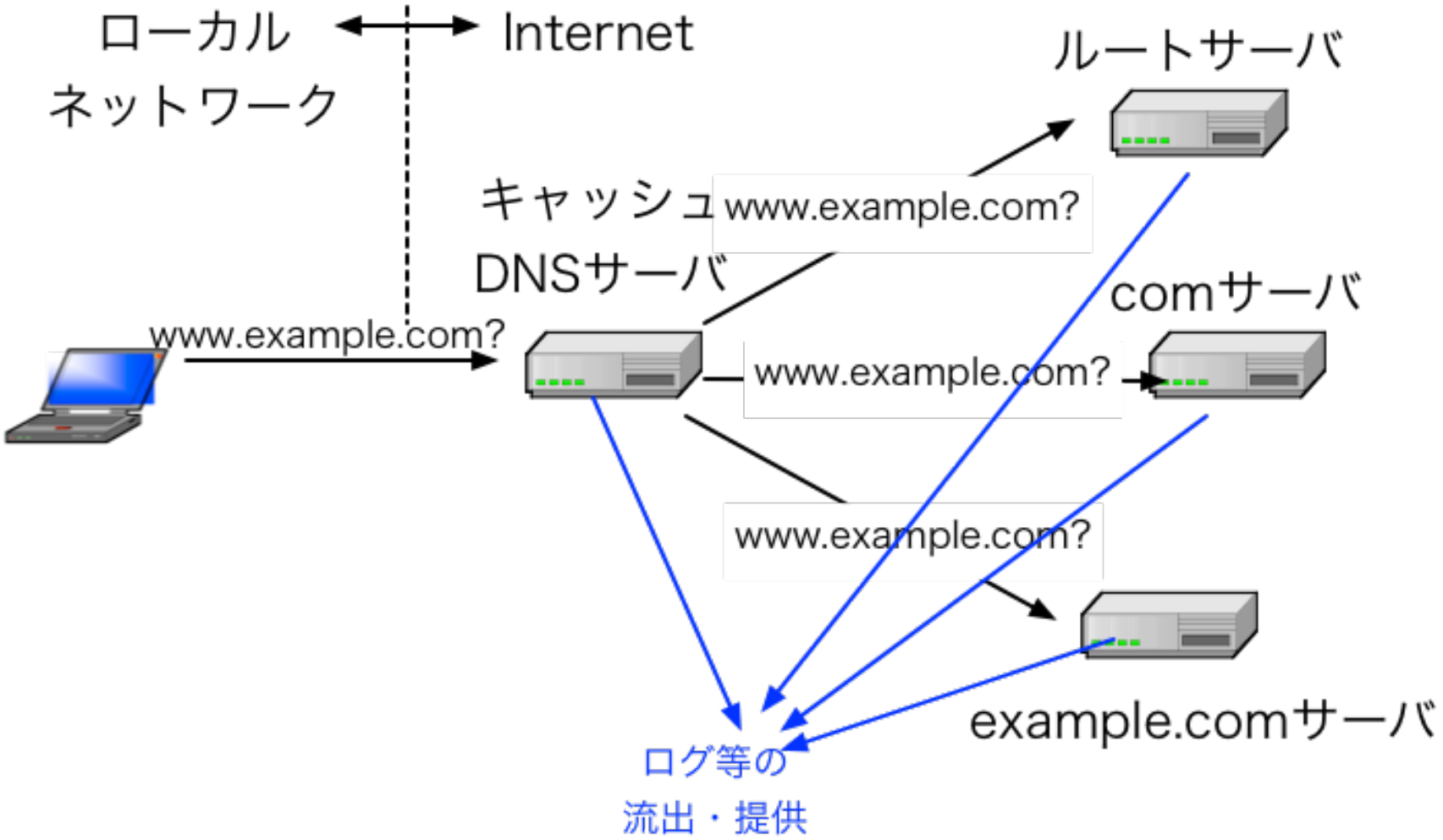
DNSプライバシー: パケット盗聴のリスク



 |

Infoblox

DNSプライバシー: データ流出のリスク



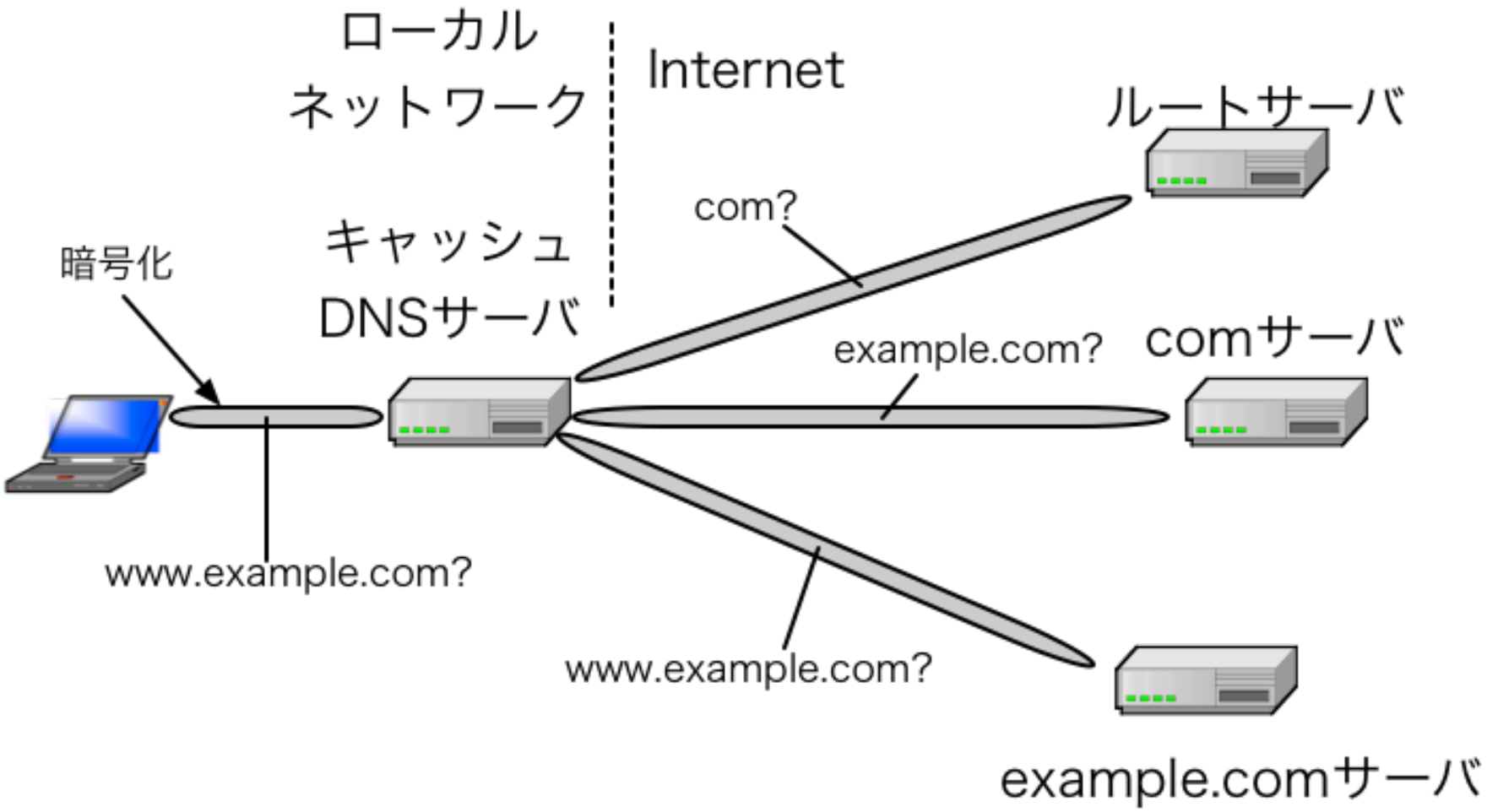
 |

Infoblox

DNSとプライバシー: 対応案

- DNSメッセージの暗号化
  - dprive IETF wgがDNS/TLSを採択
    - サーバ実装: unbound
    - クライアント実装: getdns
- ローカルネットワークでのキャッシュサーバ運用
  - サーバからの情報流出防止
- キャッシュ・権威サーバ間のクエリ名短縮
  - 例: ルートサーバにはTLDのみ問い合わせ

DNSプライバシー: 対策アーキテクチャ例



 |

Infoblox

DNSとプライバシー対策技術の影響

- クエリ短縮化によるクエリパターンの変化
  - 標準に準拠しない一部実装との間の互換性問題
  - 性能への影響(長短両面あり)
- 暗号化に伴う種々の影響(おもに性能上の負荷)
  - (TLSの場合)TCPの利用増自体による負荷
  - 暗号化自体の負荷
  - クライアントとの「セッション」を維持するための負荷

- 実際に普及するかどうかは未知数
  - 試験的実装・運用は今後でてきそう
  - 要watch

