DNSに対する脅威とその分類
～DNSセキュリティを考えるにあたって～

2014年11月20日

Internet Week 2014 チュートリアル

株式会社日本レジストリサービス（JPRS）

森下 泰宏（Yasuhiro Orange Morishita）

自己紹介

- 氏名：森下 泰宏（もりした やすひろ）
- 勤務先：（株）日本レジストリサービス
- 肩書：広報宣伝室 技術広報担当
- 主な業務内容：ドメイン名・DNSに関する技術情報をわかりやすく伝える
- 最近思うこと：今年はもうお腹いっぱいです・・・

このトラックの内容

- 目的の再確認と必要な知識のおさらい
- DNSに対する脅威（threat）の分類・整理
- 対策（defense）を考慮する上でのポイント
- DNSにおける三大事項：仕様・実装・運用
- これからの講演内容
- 有用な文献資料

このトラックの目的

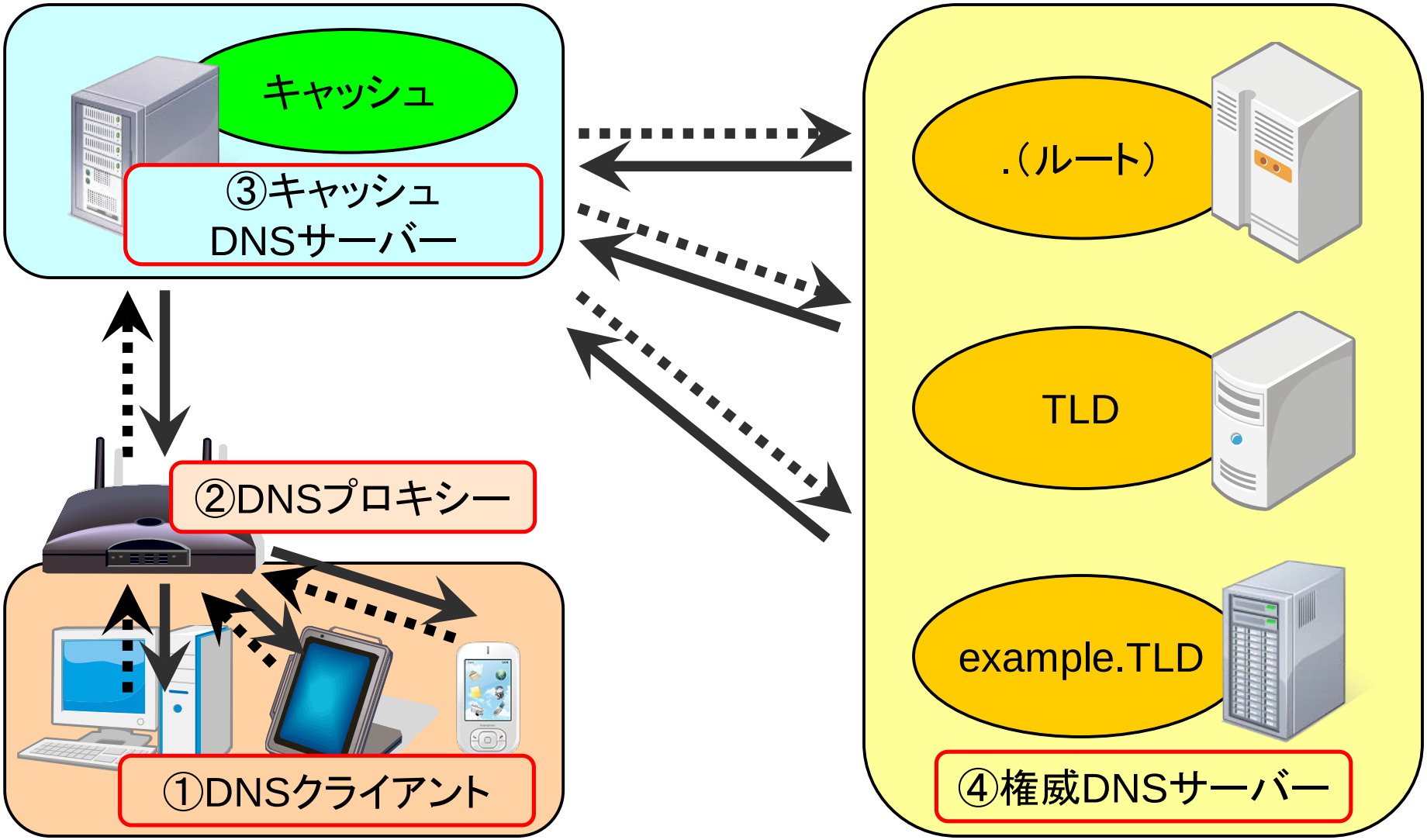
- 目的は以下の二つ
- DNSに対する脅威を分析・整理することにより、

① DNSのセキュリティを考えるにあたり必要となる、基本的な考え方を学ぶ
② 本日これから話される、DNSの「仕様」「実装」「運用」セキュリティの講演内容への橋渡しをする

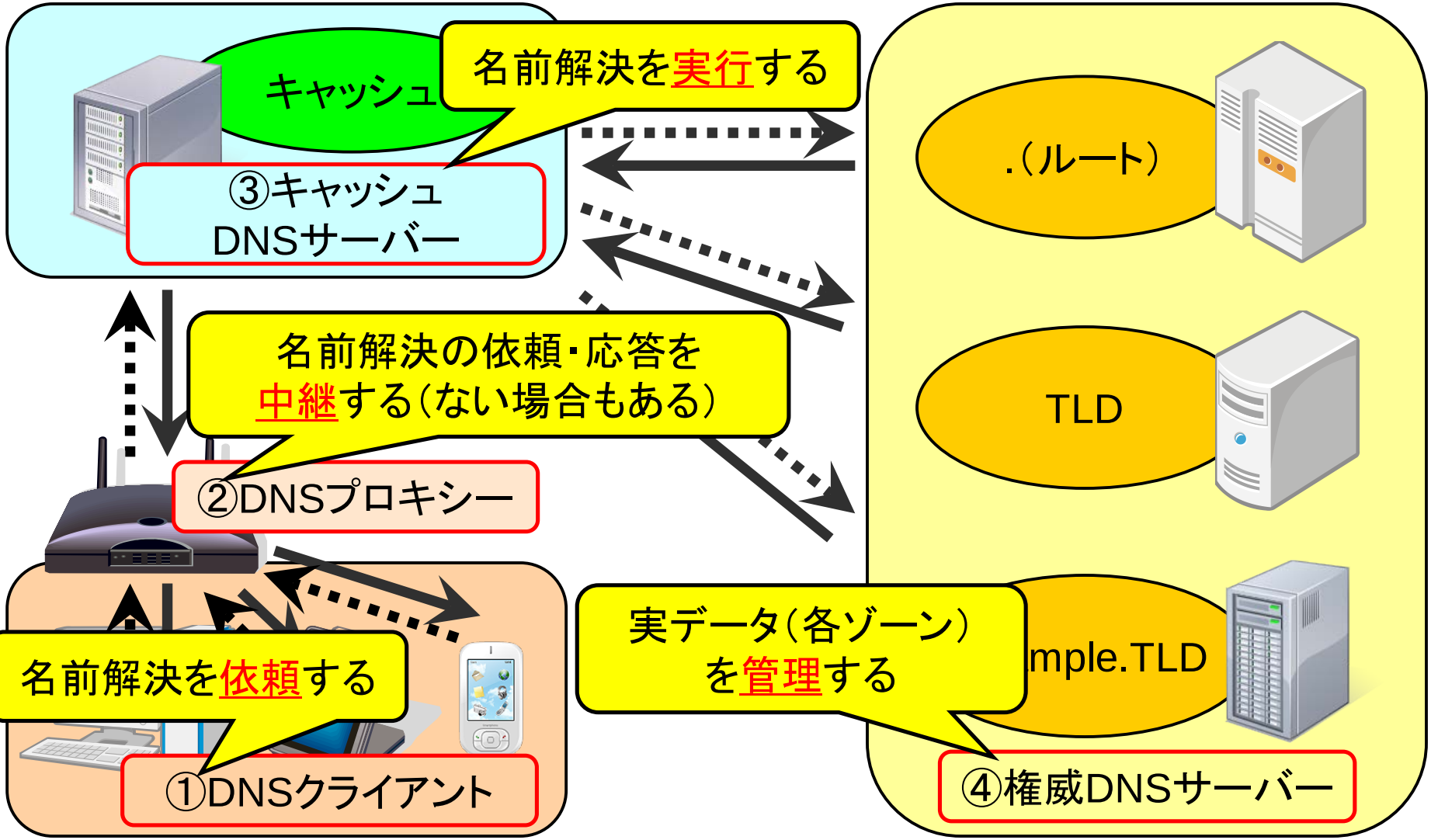
おさらい：脅威（threat）とは何か？

- エラーやトラブルの直接の原因ではないが、その要因となりうるさまざまな要素
- 実生活における脅威の例
  - あせっている、時間に追われている、長時間の連続勤務、二日酔い、寝不足など
- DNSプロトコルに対する脅威の例（RFC 3833から抜粋）
  - パケット傍受、ID・問い合わせの推測、名前の連鎖、不在証明、ワイルドカード、DNSSECの弱点

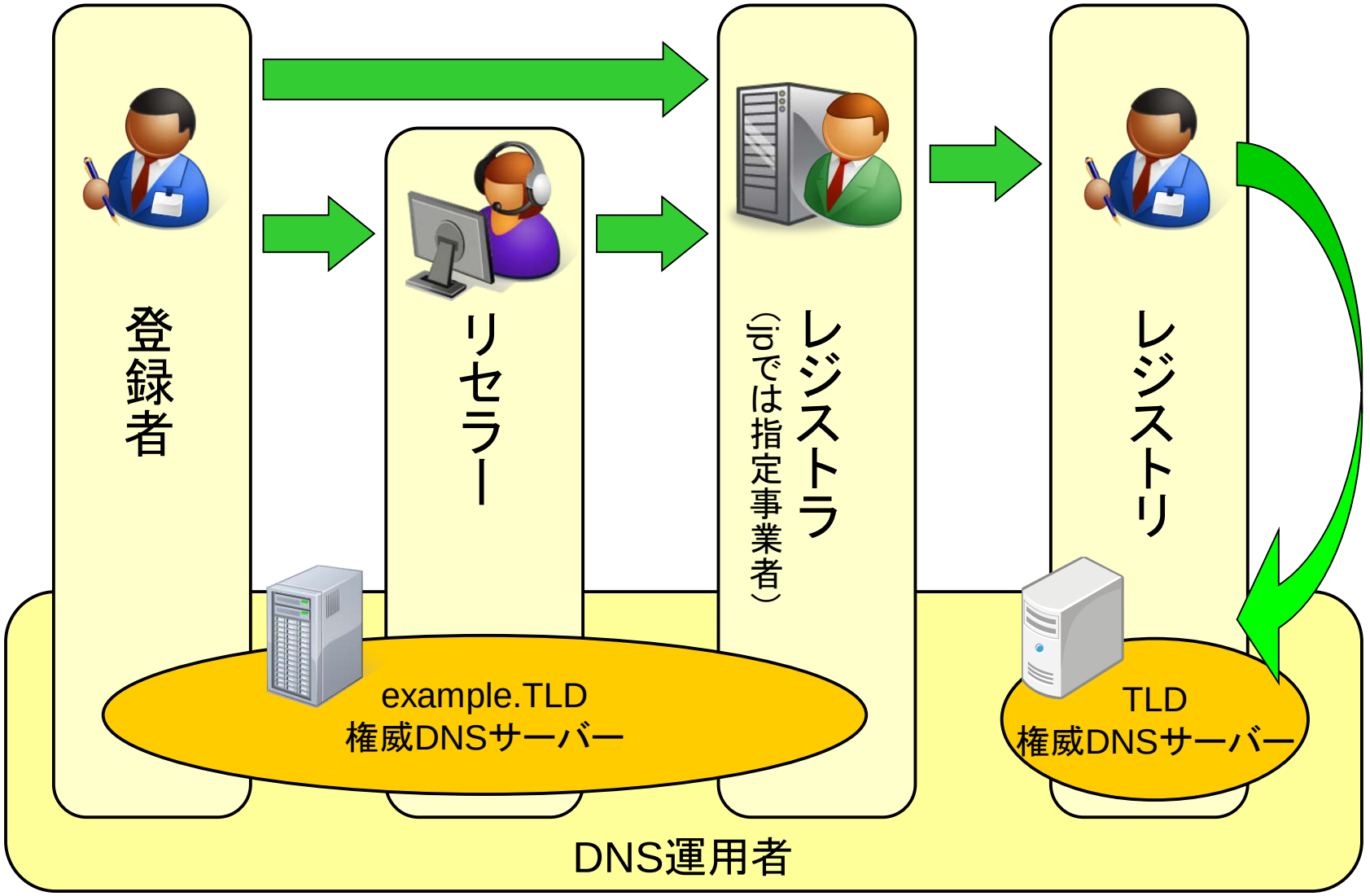
おさらい：DNSの構成要素とその役割



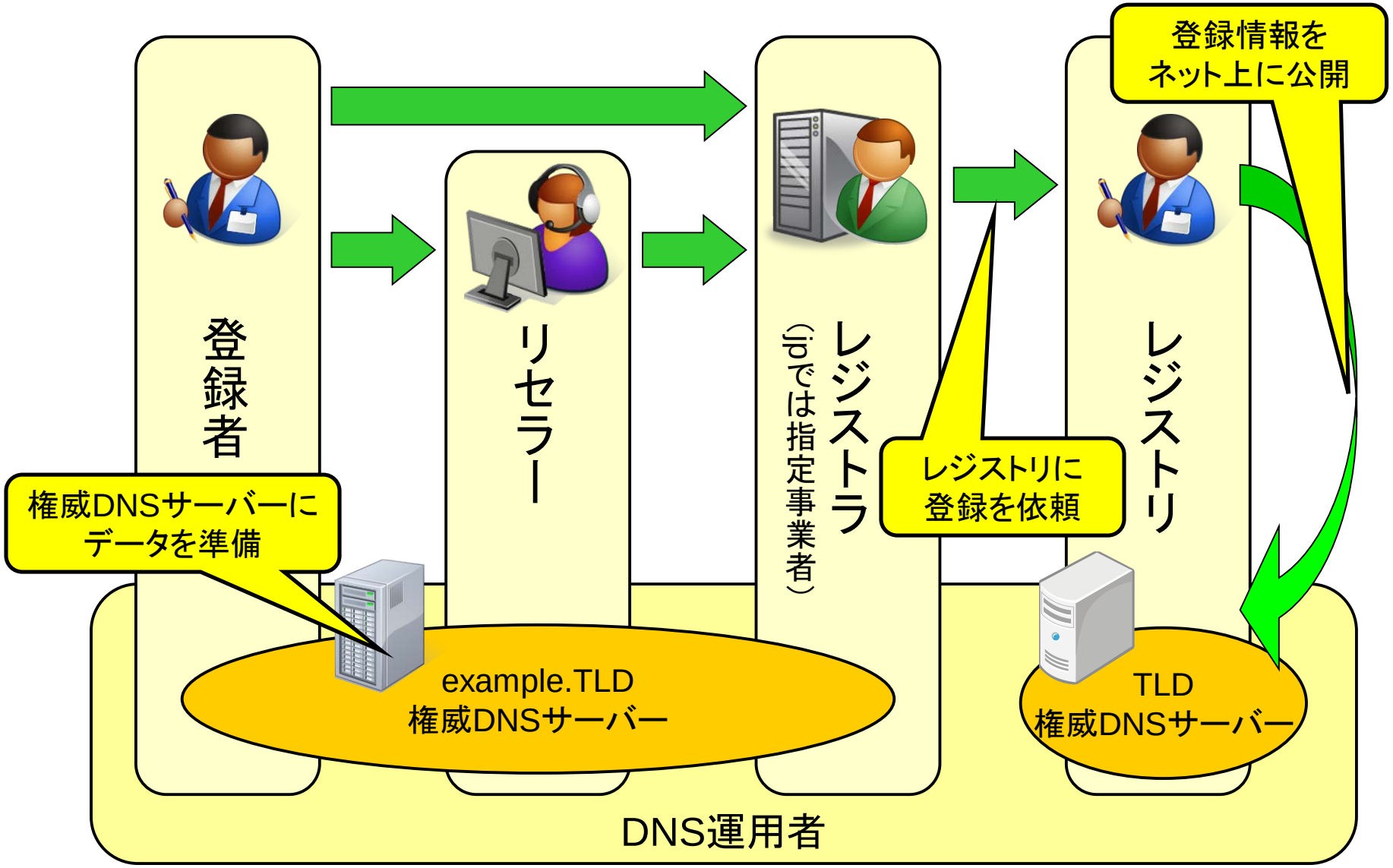
おさらい：DNSの構成要素とその役割



おさらい：DNSのデータ（登録情報）の流れ



おさらい：DNSのデータ（登録情報）の流れ



脅威を分類・整理する際のポイント

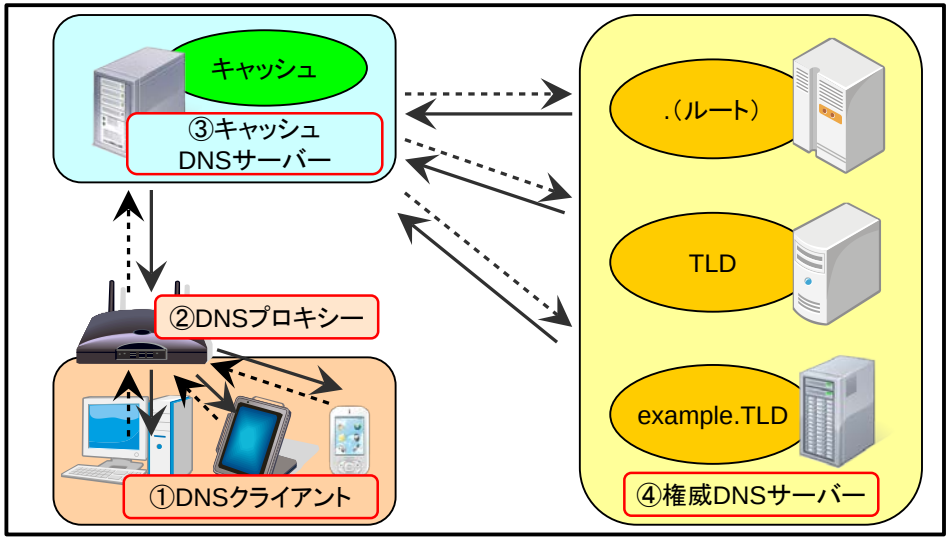
- 脅威を分類・整理する際の二つのポイント

① それは何に対する脅威か？
② その脅威を狙う攻撃の効果（攻撃者の意図）は何か？

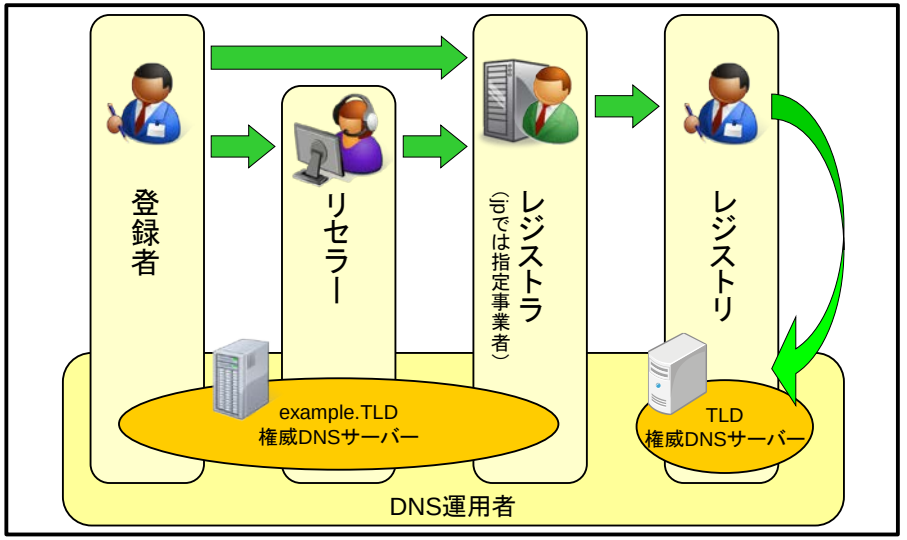
- 特に、DNSにおける脅威を分類・整理する場合、DNSの構成要素とDNSデータ（登録情報）の双方について考慮する必要があることに注意が必要

DNSに対する脅威の分類・整理
①それは何に対する脅威か？

- DNSの構成要素に対する脅威
  - DNSの構成要素が攻撃対象となる（左図）
- DNSのデータに対する脅威
  - DNSに登録される情報が攻撃対象となる（右図）

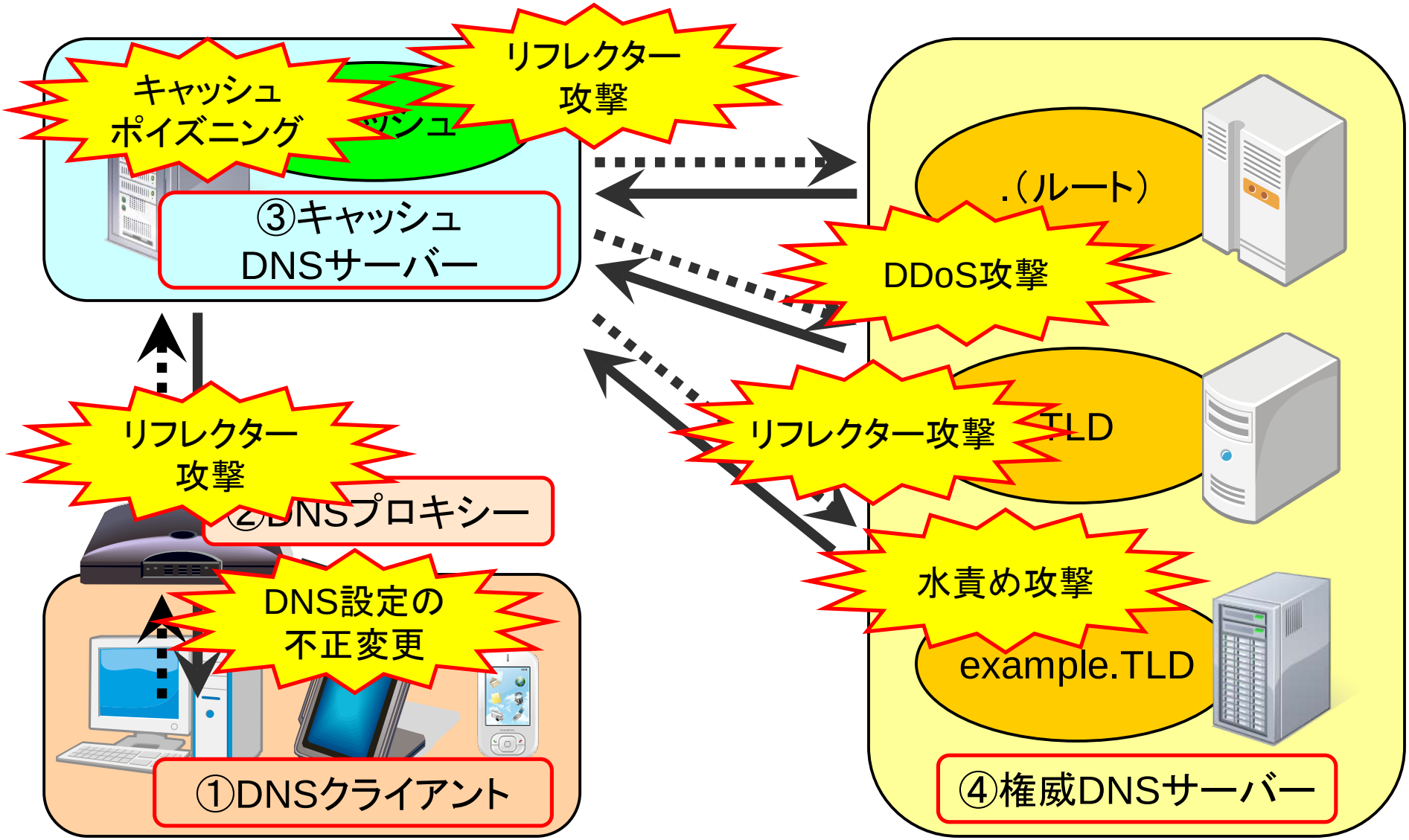


DNSの構成要素が攻撃対象

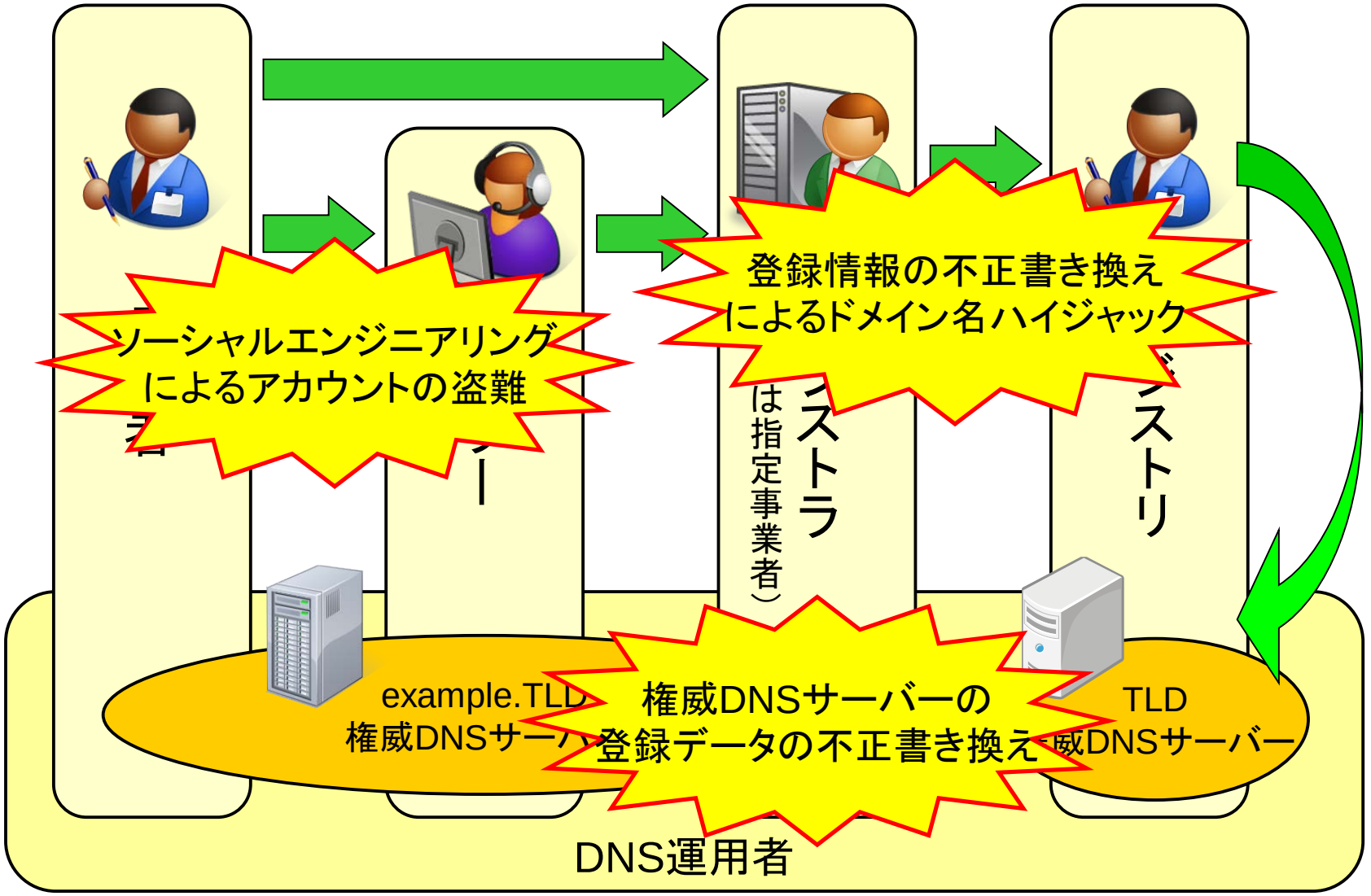


DNSに登録される情報が攻撃対象

DNSの構成要素に対する攻撃の例



DNSのデータに対する攻撃の例



DNSに対する脅威の分類・整理
②その攻撃の効果（攻撃者の意図）は何か？

- DNSを使わせない（DoS）
  - 例：DNS水責め攻撃、サーバーの脆弱性を突いた攻撃
- 偽のDNSデータを使わせる
  - 例：キャッシュポイズニング、ドメイン名ハイジャック
- DNSを攻撃の手段として利用する
  - 例：DNSリフレクター攻撃
- DNSの情報を不正に入手する
  - 例：不正なゾーン転送要求・ゾーン列挙・キャッシュ覗き

攻撃の狙いは何で、何が脅威にさらされるかの把握が重要

対策（defense）を考慮する上でのポイント

- 今、どんな脅威にさらされているのか
  - とるべき対策やその優先度を考える上での出発点
- その対策で「何から」「何を」「どう」守るか
  - 何から：想定される脅威の明確化
  - 何を：守るべきターゲットの明確化
  - どう：投入すべき手法や構築すべき体制の明確化
- その対策で「守れること」と「守れないこと」は何か
  - 対策の有効範囲の明確化

これらを考慮しなければ、有効な対策をとれない

DNSにおける三大事項：仕様・実装・運用

- 仕様（specification）
  - プロトコルにおける多くの不明瞭点・弱点の存在
  - 既存実装への影響・後方互換性の考慮の必要性
- 実装（implementation）
  - 実装における裁量（判断要素）の多さ
  - 実装におけるデファクトスタンダードの存在
- 運用（operation）
  - 運用が仕様や実装に与える影響の大きさ
  - ポリシーが運用に与える影響の大きさ

DNSでは、これらを常に組み合わせて考慮する必要がある
これはDNSセキュリティにおいても同様

これからの講演内容

- 各エキスパートがそれぞれの事項について解説
  - 仕様（基本仕様とキャッシュポイズニングを題材に）
    - 株式会社インターネットイニシアティブ：其田学さん
  - 実装（ホームルーターにおける事例を題材に）
    - NECプラットフォームズ株式会社：川島正伸さん
  - 運用（ドメイン名とDNSの運用を題材に）
    - 株式会社日本レジストリサービス：阿波連良尚さん

参考：有用な文献資料（1/2）

- RFC 3833: Threat Analysis of the Domain Name System (DNS)

  <https://tools.ietf.org/html/rfc3833>

  – DNSプロトコル上の脅威を文書化し、それに対する防御手段としてのDNSSECの有効範囲を考察したもの

  – DNSSECを含むDNSのセキュリティについて考える際のベースとなる文書、一読を強く推奨

  – JPRSで日本語訳を公開

    - DNS(Domain Name System)の脅威分析

      <http://jprs.jp/tech/material/rfc/RFC3833-ja.txt>

参考:有用な文献資料(2/2)

- DNS Threat Analysis - NLnet Labs document 2006-SE-01 version 1.0

  <http://www.nlnetlabs.nl/downloads/se-consult.pdf>

  – DNS全般に対する脅威について分析し、それに対応するために必要な推奨事項を網羅的にまとめたもの

  – よく書かれており、一読を強く推奨

  – PDFで27ページ、かなりのボリューム

    - 目次(全体構成)・4ページの図(Attack Tree)・本文中の「Recommendations」の各項目に目を通しておくとよい

That’s it!