DNSセキュリティ最新動向
～対策の基本と最近の攻撃手法～

2015年2月7日
SECCON 2014 全国大会カンファレンス
株式会社日本レジストリサービス（JPRS）
森下 泰宏（Yasuhiro Orange Morishita）
@OrangeMorishita

自己紹介

- 氏名：森下 泰宏（もりした やすひろ）
- 勤務先：株式会社日本レジストリサービス
- 肩書：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
- 一言：昨年はほんとに「お腹いっぱい」でした・・・
  - セキュリティ関係のイベント・事件が目白押しでした

JPRSとは？

- 正式名：株式会社日本レジストリサービス
  - 英文名称：Japan Registry Services Co. Ltd.
  - 略称：JPRS（ジェーピーアールエス）
- 「ドメイン名レジストリ」という組織の一つ
  - ドメイン名業界では単に「レジストリ」と呼ばれている
- 「日本」に割り当てられているccTLD「jp」を管理
  - ccTLD：国コードトップレベルドメイン
  - 例：seccon.jp, jprs.co.jp, dendai.ac.jp, ...

JPRSは国コードトップレベルドメイン（ccTLD）「jp」のレジストリ

ドメイン名レジストリの役割

- あるドメイン名（例：jp）に対し、一つ存在
- レジストリの二つの重要な役割
  - ドメイン名の登録を受けつけ、それを誰（組織・個人）が使っているか、という情報を管理する
  - DNSという仕組みの、重要な一部分を管理運用する
    - 具体的にはそのドメイン名の「権威DNSサーバー」
- つまり、JPRSは・・・

ccTLD「jp」を管理し、インターネットで使えるようにしている会社

JPRSとSECCONの関係

- SECCON 2014（今年度）から協賛
- SECCON 2014長野大会
  「DNS Security Challenge」に特別協賛
  - 2014年9月27～28日 at 信州大学工学部
- 長野大会の問題作成と当日の大会運営をサポート
  - 「DNS攻撃パケット解析」「DNS早押しクイズ」
    - 攻撃パターン作成の監修
    - クイズ問題の作成と当日の読み上げ
  - 講演を担当
    - 30分で学ぶDNSの基礎の基礎
    - DNS水責め攻撃の概要

長野大会の様子

本日の内容

1. DNSセキュリティにおける基本的な考え方
   ① DNSに対する脅威とその分類
   ② 対策（defense）を考慮する上でのポイント
   ③ DNSにおける三大事項：仕様・実装・運用
2. 最近話題になっている攻撃の概要とその対策
   ① DNS水責め攻撃
   ② 登録情報の不正書き換えによる
   ドメイン名ハイジャック

1. DNSセキュリティにおける基本的な考え方

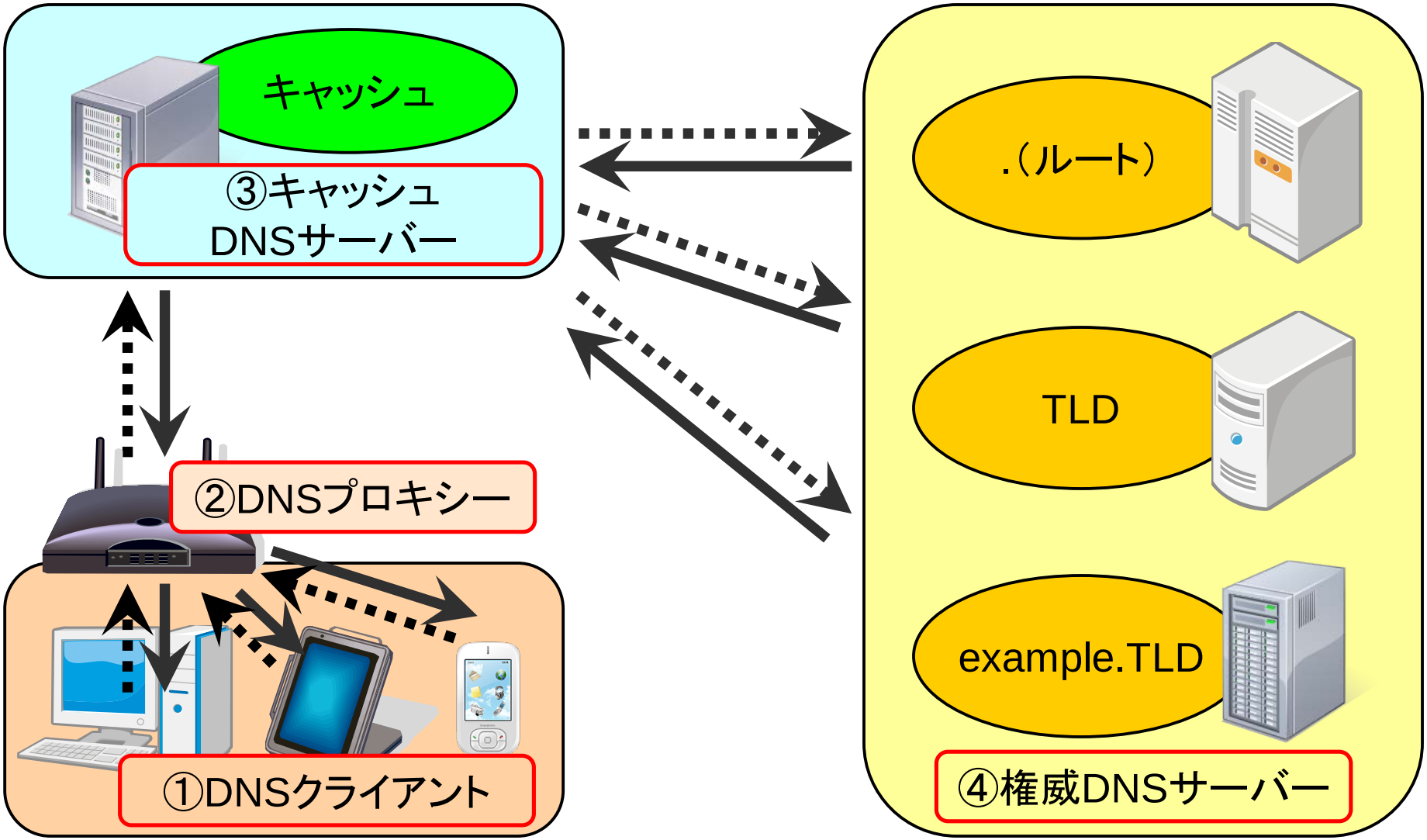
このパートの構成

- 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

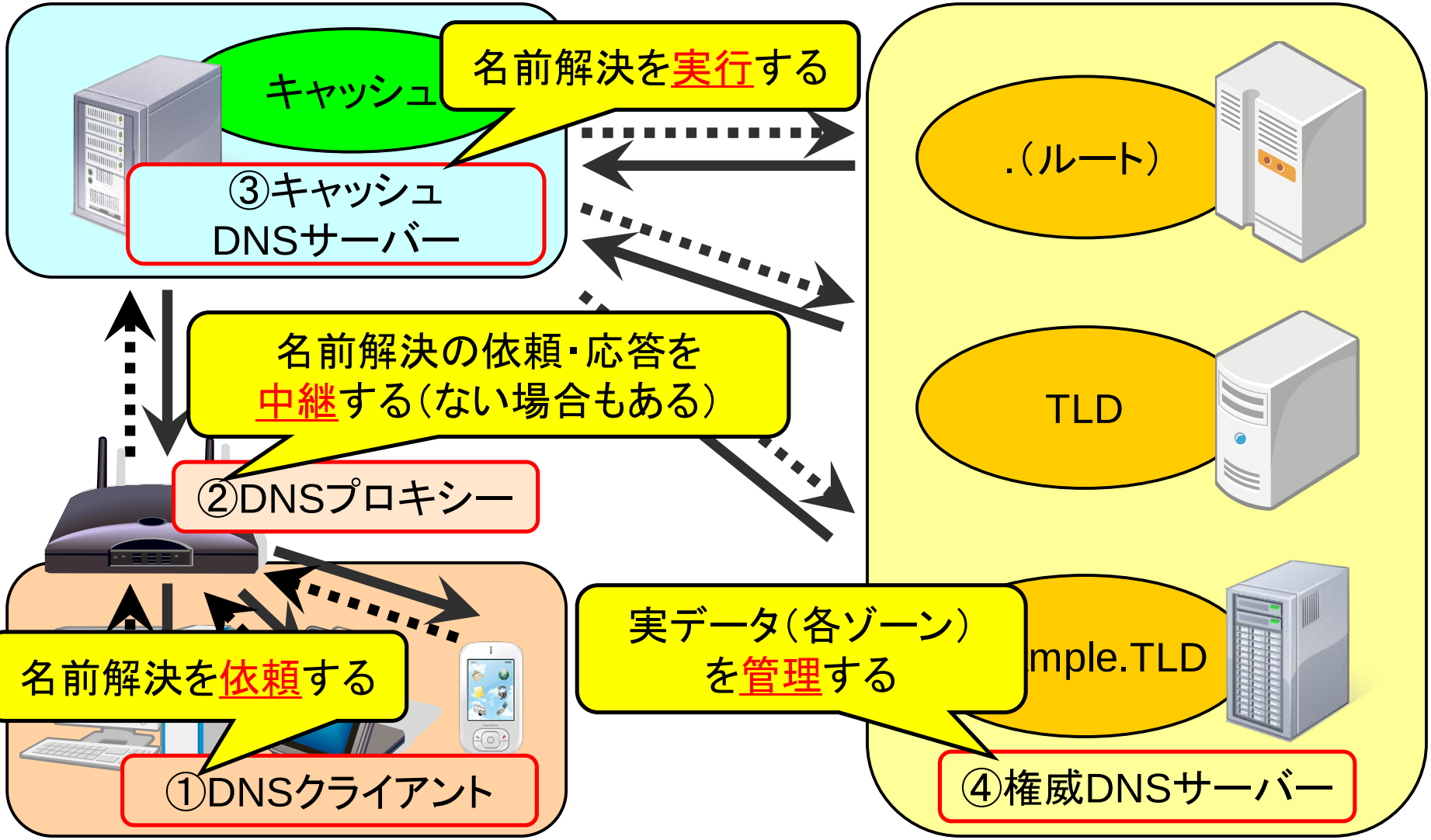
おさらい：脅威（threat）とは何か？

- 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

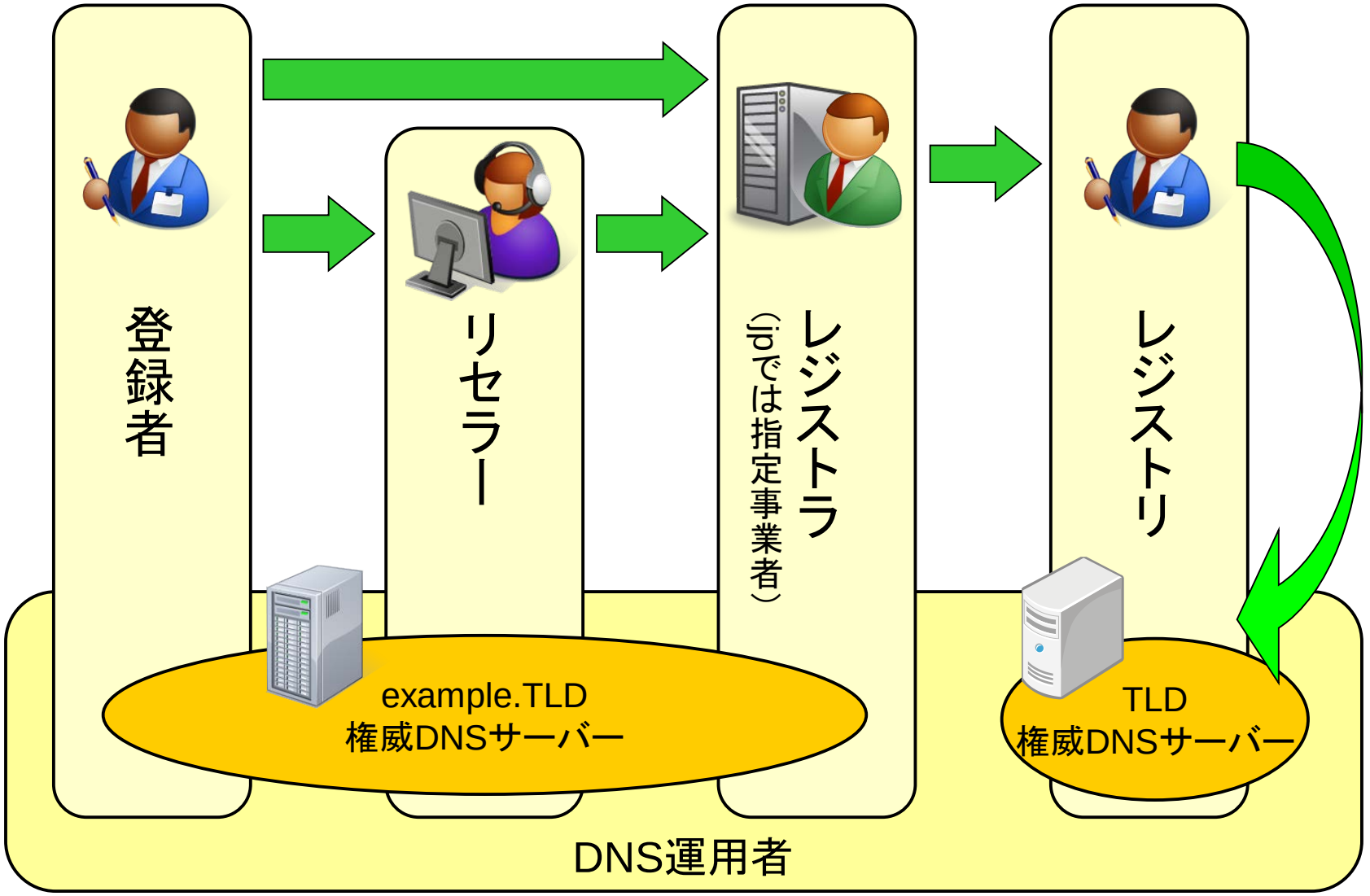
おさらい：DNSの構成要素とその役割



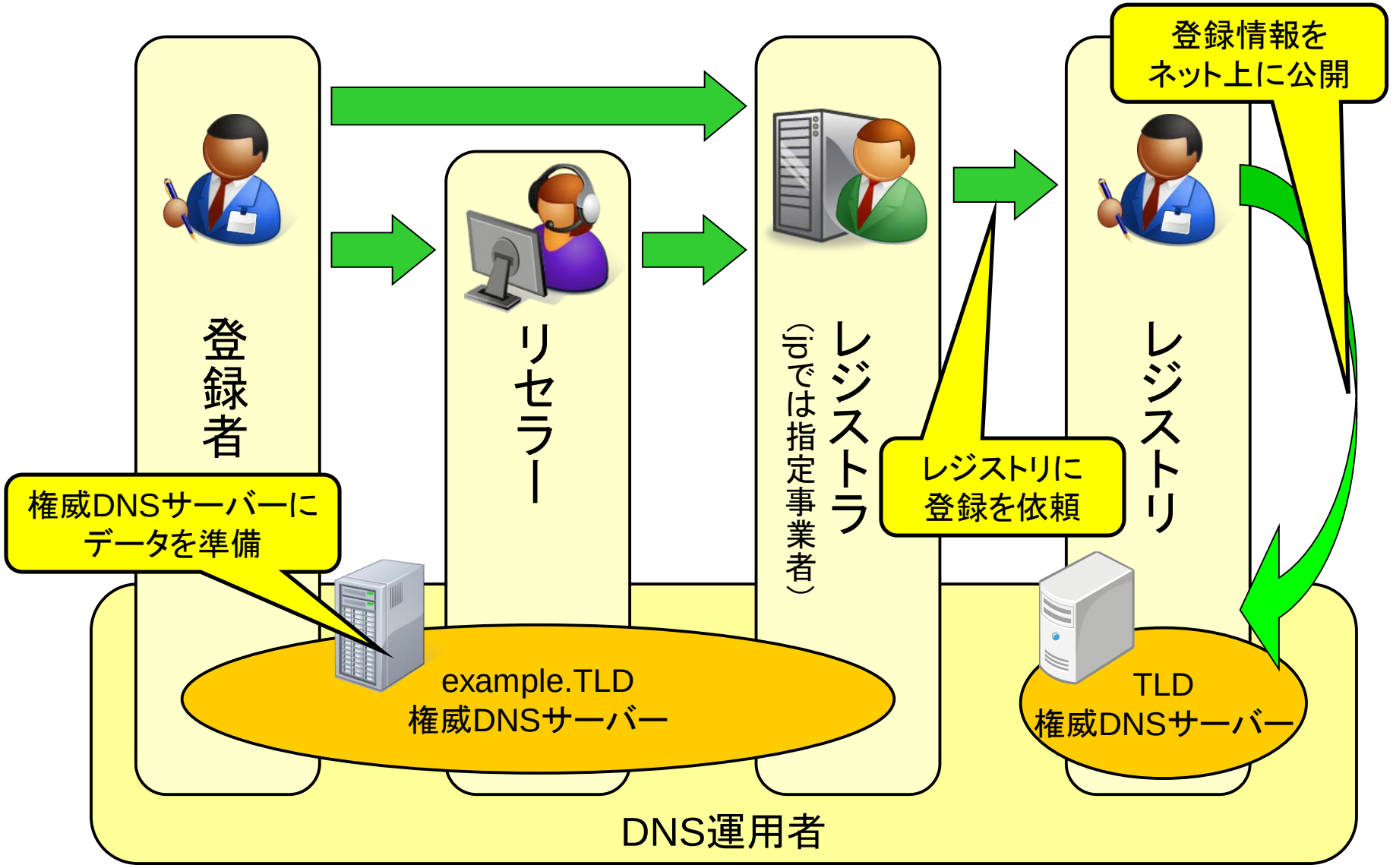
おさらい：DNSの構成要素とその役割



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

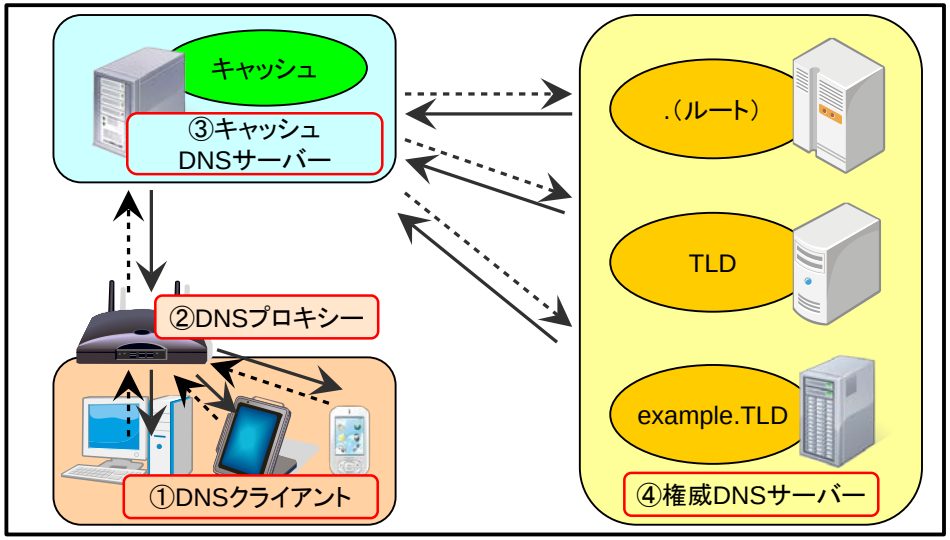
- 脅威を分類・整理する際の二つのポイント

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？

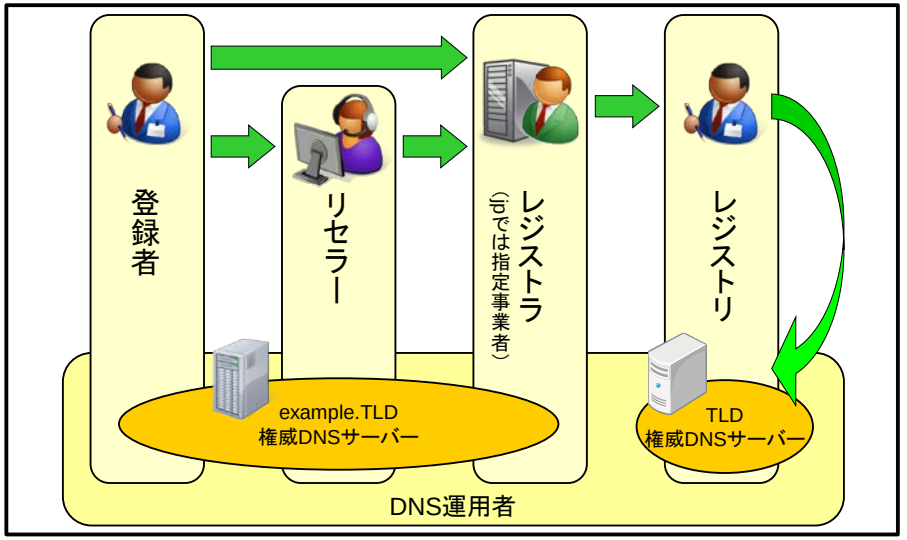
- 特に、DNSにおける脅威を分類・整理する場合、DNSの構成要素とDNSデータ（登録情報）の双方について考慮する必要があることに注意が必要

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）

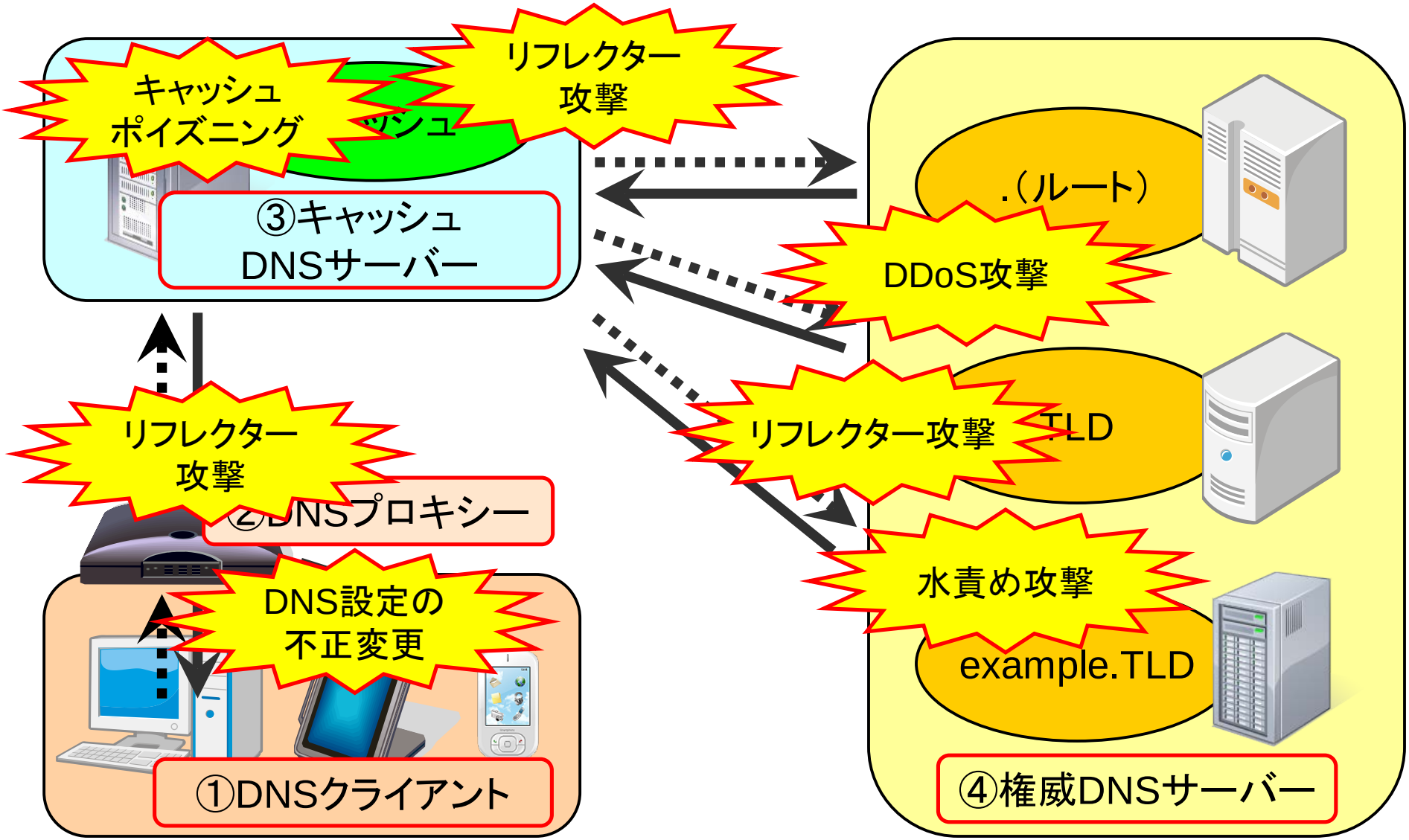


DNSの構成要素が攻撃対象

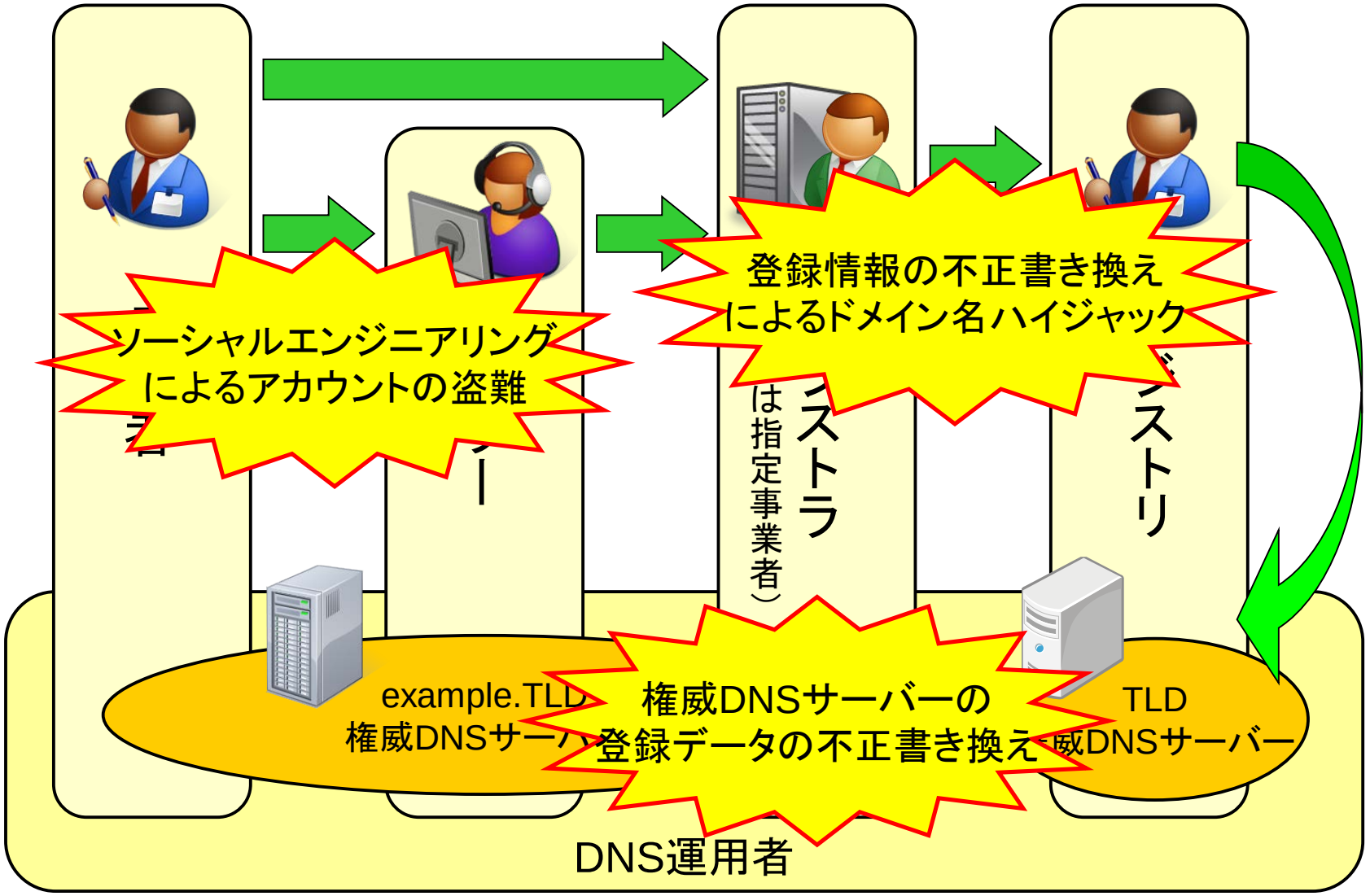


DNSに登録される情報が攻撃対象

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

2. 最近話題になっている攻撃の概要とその対策

①DNS水責め攻撃

このパートの構成

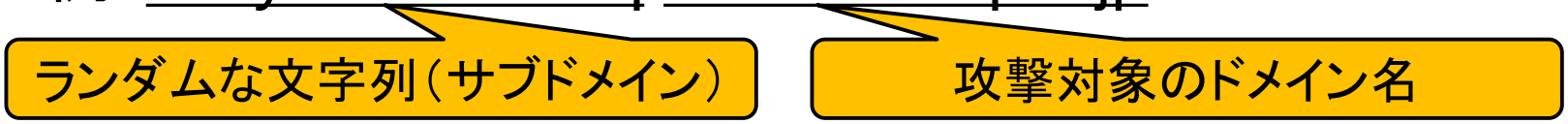
- 攻撃の特徴
- 攻撃の目的
- 攻撃名称の由来
- 攻撃のシナリオ
- 攻撃成立の理由
- 取りうる攻撃対策
- この攻撃における注意点

攻撃の特徴(1/2)

- 2014年1～2月頃から世界的に観測され始めた、DNSサーバーに対するDDoS攻撃の手法
  - 攻撃は現在も行われている
- 第三者のオープンリゾルバーやホームルーターを、攻撃の踏み台として悪用している
- しかし、DNS応答を攻撃に使っておらず、いわゆるDNSリフレクター(DNS Amp)攻撃ではない
  - この攻撃では送信元IPアドレスの詐称は必須ではない

攻撃の特徴(2/2)

- 攻撃対象のランダムなサブドメインの問い合わせが、キャッシュ／権威DNSサーバーに大量に到達
  - 例：asdykuadkncezq.www.example.jpのAレコード



  - 「ランダムDNSクエリー攻撃」「ランダムサブドメイン攻撃」などとも呼ばれている
- カミンスキー型攻撃手法の問い合わせと同一
- しかし、カミンスキー型攻撃手法で検出されるはずの、問い合わせに対応する偽の応答が検出されない
  - そのため、発生当初は攻撃の目的が判然としなかった

攻撃の目的(と考えられていること)

- 攻撃対象ドメイン名の権威DNSサーバーが、真の攻撃対象であったと考えられている
  - 攻撃対象ドメイン名の権威DNSサーバーを過負荷にし、攻撃対象サイトをアクセス不能の状態に陥らせる
- 有力な状況証拠
  - 攻撃対象になった数百のドメイン名の多くが、中国・台湾・香港関係のECサイトやカジノサイトなどの中華系の金が動くサイトであったと報告されている
  - 香港の雨傘革命の活動状況を報道したニュースサイトが、攻撃対象になったという情報がある

被害が出た国内ISPは、真の攻撃目標ではなかった？

- 5月から7月にかけ、国内の複数のISPにおいて「DDoS攻撃によるDNSの障害」が相次いで発生
  - この攻撃の巻き添えを食ったと言われている
  - 巻き添えが起こる仕組みについては後述
- 関係者によると、攻撃はその後も観測されているとのこと

なぜ「水責め」と呼ばれるのか？

- 2014年2月にこの攻撃を報告した米国Secure64 Softwareが、公式ブログで命名
  - Water Torture: A Slow Drip DNS DDoS Attack
    <https://blog.secure64.com/?p=377>
    - Water Torture = 水責め（水攻めではないので注意）
- dns-operations MLでの関係者の発言やSecure64 Softwareの技術者から得た回答によると、「水責め」、特に「中国式水責め」に由来しているとのこと

「中国式水責め」

- Wikipedia英語版：Chinese water torture
  <http://en.wikipedia.org/wiki/Chinese_water_torture>

> “Chinese water torture is a process in which water is slowly dripped onto a person's forehead, allegedly driving the restrained victim insane.”

（椅子に相手を縛り付け、額にゆっくりと水滴を滴下する）

- 今回の攻撃形態や、攻撃により各DNSサーバーが徐々に追い込まれていくさまが、<u>この手法を彷彿（ほうふつ）とさせる</u>
  - 多数のBot（送信元IPアドレス）を用いた低頻度の攻撃

攻撃のシナリオ：登場人物

①攻撃者

オープンリゾルバーのリスト

②Botnet

③オープンリゾルバー

⑥攻撃対象ドメイン名の権威DNSサーバー

ns1

ns2

ISP A

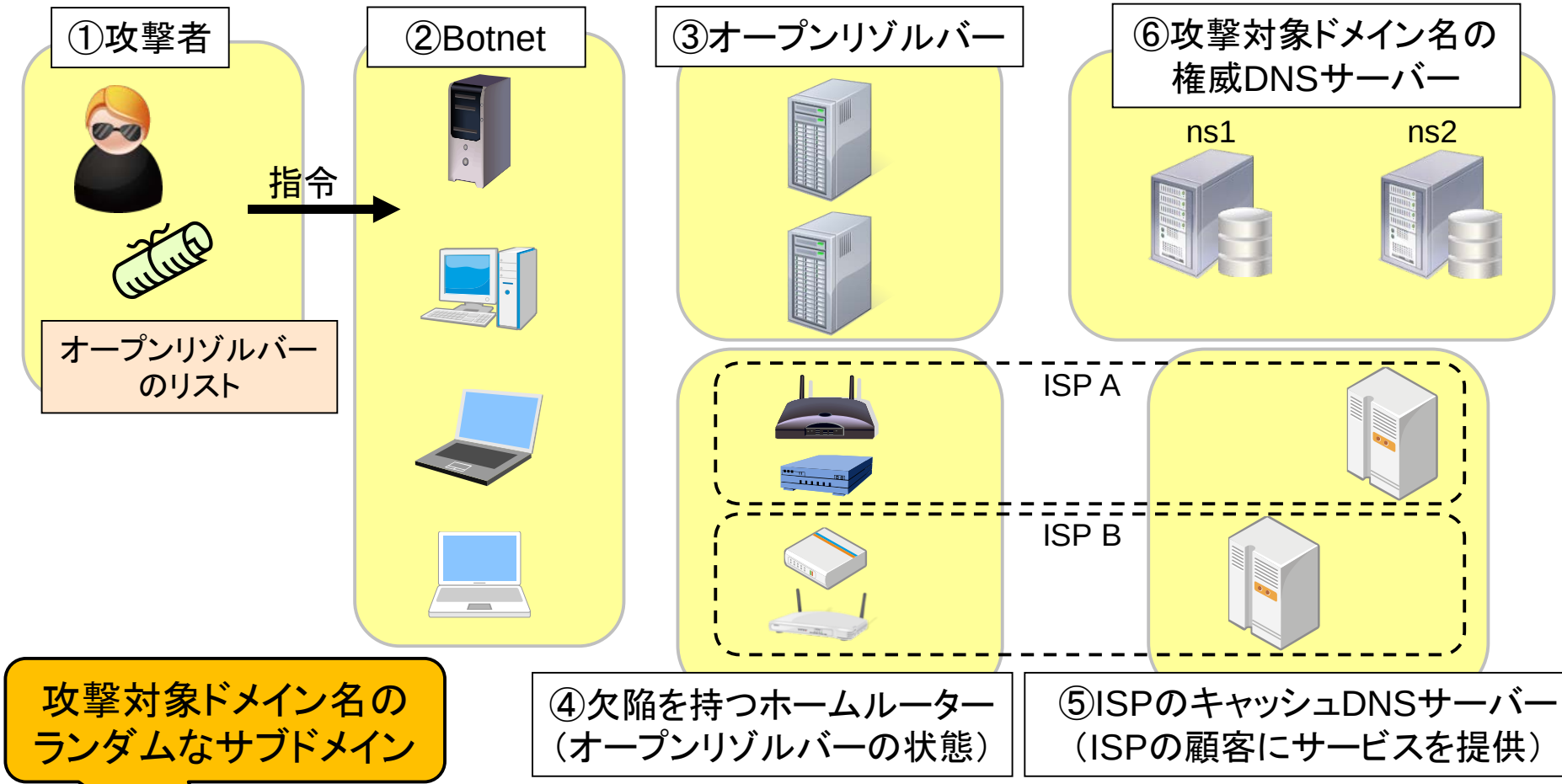
ISP B

④欠陥を持つホームルーター（オープンリゾルバーの状態）

⑤ISPのキャッシュDNSサーバー（ISPの顧客にサービスを提供）

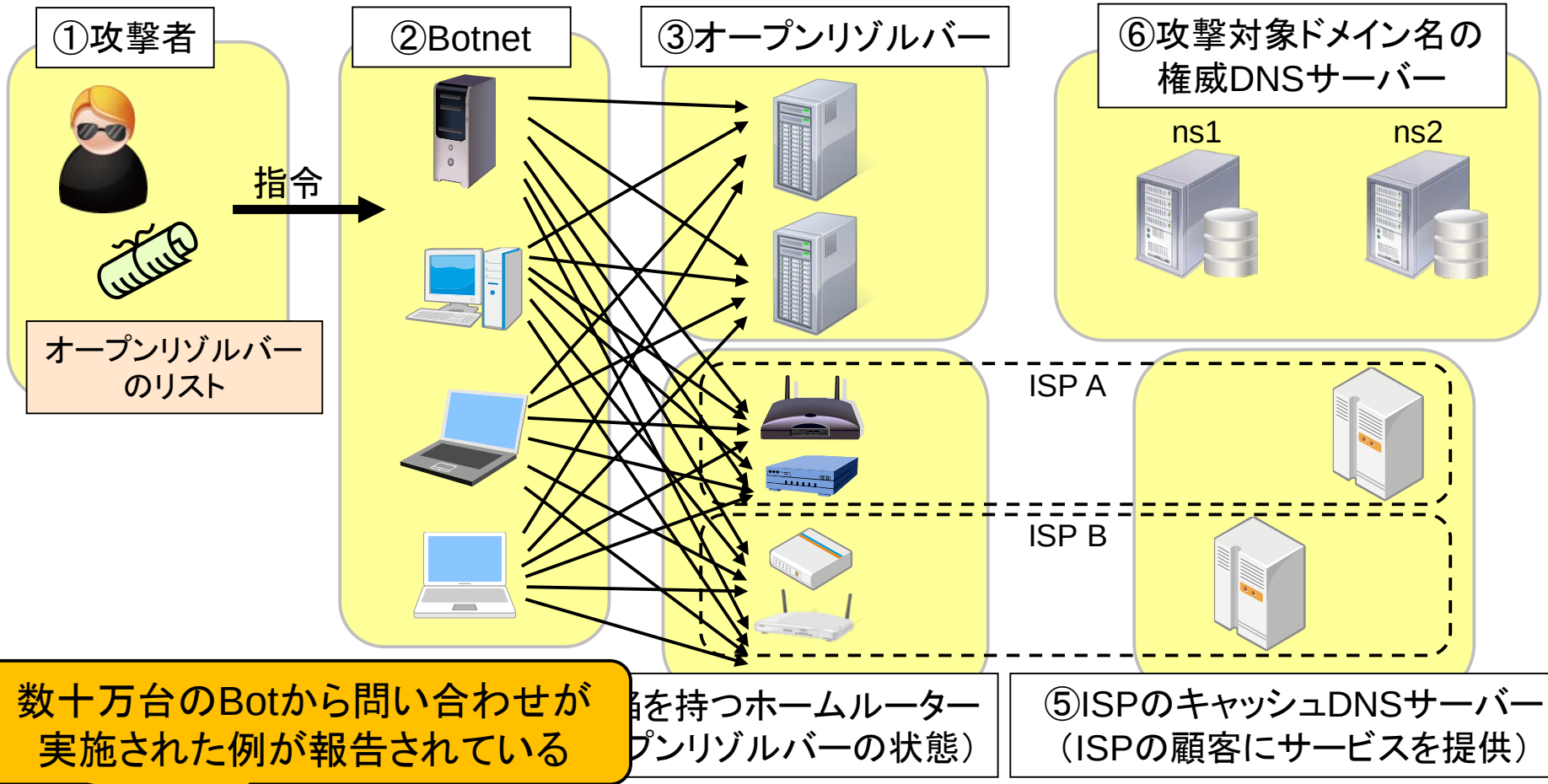
登場人物は大きく分けて6種類

攻撃のシナリオ（1/4）



1. 攻撃者がBotnetに、リストにあるオープンリゾルバーに対して (random).www.example.*TLD*をDNS問い合わせするように指令を出す

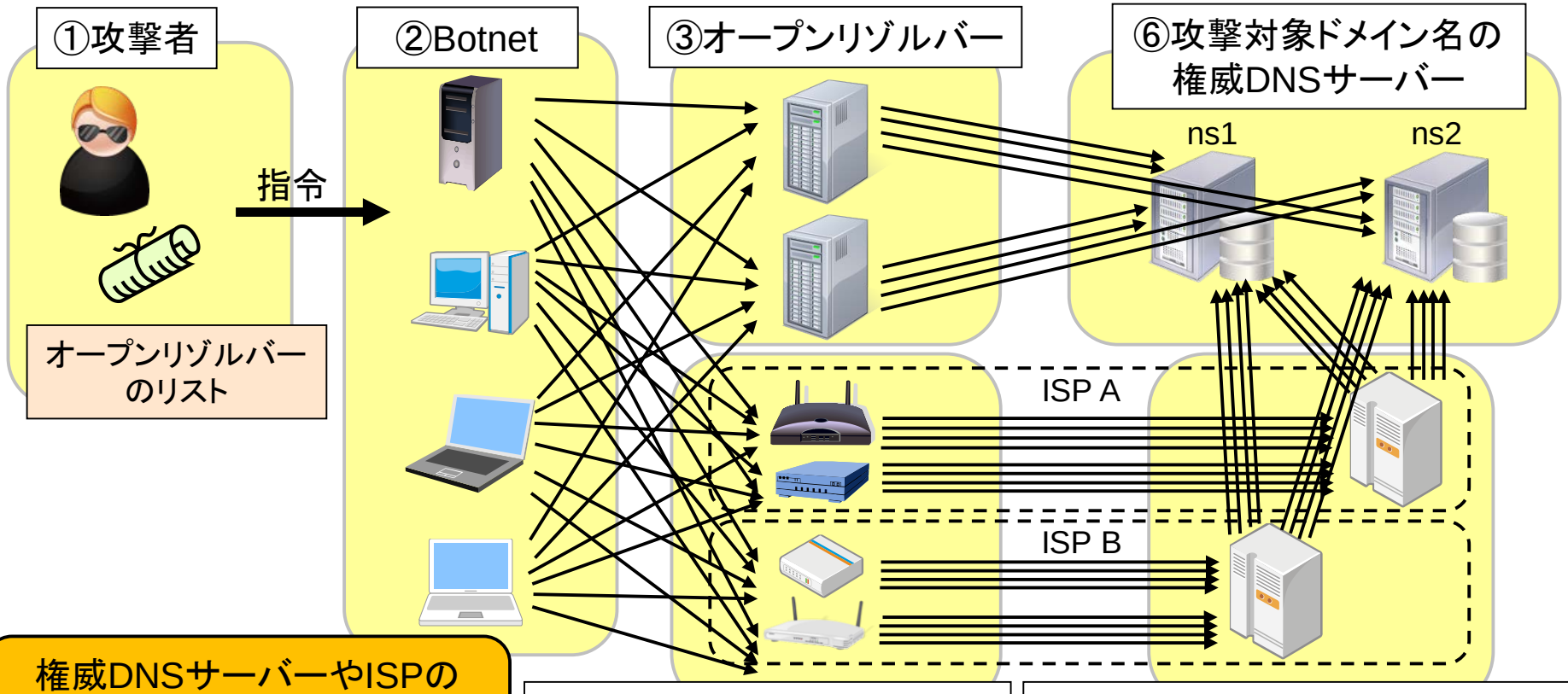
攻撃のシナリオ（2/4）



数十万台のBotから問い合わせが実施された例が報告されている

2. Botnetを構成する各PC（Bot）が、リストに掲載されたIPアドレスに問い合わせを送る
規制回避のため、数多くのBotから「広く薄く」問い合わせが送られる（Slow Drip）

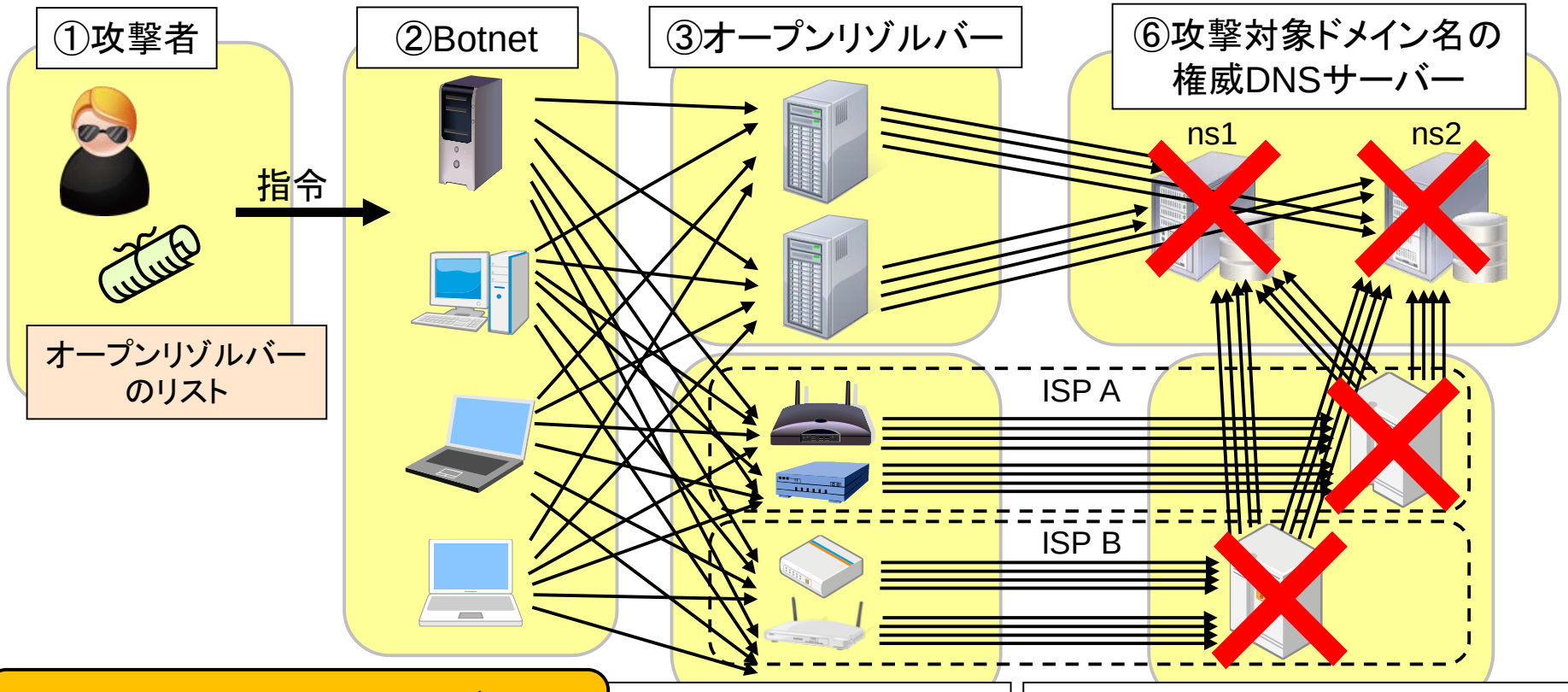
攻撃のシナリオ（3/4）



権威DNSサーバーやISPのキャッシュDNSサーバーにアクセスが集中する

3. キャッシュに存在しないため、権威DNSサーバーに問い合わせが毎回発生
（ホームルーターではISPのキャッシュDNSサーバーに問い合わせが毎回転送）

攻撃のシナリオ（4/4）



ISPのキャッシュDNSサーバーは、顧客側から攻撃されることになる

4. 問い合わせが集中する攻撃対象ドメイン名の権威DNSサーバーやISPのキャッシュDNSサーバーが過負荷になり、サービス不能状態に陥る

攻撃成立の理由

- 存在しない・キャッシュにない名前の処理はコスト高
  - 権威・キャッシュのいずれにとっても（特にキャッシュ）
  - 「キャッシュが効かないとどうなるか」を端的に表している
- 権威DNSサーバーの過負荷（応答遅延・無応答）が、キャッシュDNSサーバーにも悪影響を及ぼす
  - タイムアウトを待ったり、再送したり、別サーバーへの問い合わせを実施したりしなければならない
    - 処理中のセッションが溜まっていく
    - 限度を超えると、問い合わせを受け付けなくなる実装がある
- Botからの直接攻撃に比べ、フィルターしにくい
  - 正規のキャッシュDNSサーバーからのアクセスであるため

取りうる攻撃対策(1/3)
キャッシュDNSサーバーにおける対策例

- 攻撃対象のゾーンをローカルに持たせる
  - 例:対象ドメイン名のIPアドレスとして127.0.0.1を指定
    - 対象ドメイン名に対するDoSは成立していることに注意
- BIND 9のRPZ(Response Policy Zone)機能を用い、「*.攻撃対象ドメイン名」の問い合わせに関する特別ルールを記述する
- iptables、あるいはそれに相当する機能でマッチングルールを書き、当該のDNS問い合わせを捨てる
  - 上記二つの対策も対象ドメイン名のDoSを成立させてしまう

決定打と考えられる対策はまだ存在しない

取りうる攻撃対策(2/3)
ISPの網側における対策例

- IP53B(外部から53/udpへのアクセスをブロック)
  - ホームルーターの欠陥を外部から利用できなくする
  - リフレクター攻撃対策として、IP123B(NTP)と共に導入が図られつつある
    - 注意:IP123Bでは、123/udp⇔123/udpという通信が発生しうることに配慮する必要がある
- 「通信の秘密」との関係を考慮する必要あり
  - 2014年7月22日にJAIPAなど5団体による「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」が改定された

取りうる攻撃対策(3/3)
プログラムの追加導入・機能追加

- いくつかの対策用プログラムが発表されている
  - 「攻撃の検知」と「対応の自動化」を図るものが多い
    - dns_servfail_attack_mitigator
      - <https://github.com/cejennings/dns_servfail_attack_mitigator>
    - unbound-reqmon
      - <https://github.com/tarko/unbound-reqmon>
    - dnsbff
      - <https://github.com/willt/dnsbff>
- BIND 9.11でExperimentalな実装が入る見込み
  - Subscription(有償)版のBIND 9でその一部が実装

この攻撃の注意点(1/2)

- この攻撃手法は単純かつ応用範囲が広い
  - DNSの仕組みそのものを攻撃に悪用している
  - キャッシュDNSサーバーへのDoSを目的にできうる
  - オープンリゾルバー経由やホームルーター経由でなくても成立しうる(クライアントPCのマルウェア経由など)
- 不用意な対策が悪影響を及ぼす場合がある
  - キャッシュDNSサーバーにおける対策により、攻撃対象ドメインへのDoSが成立してしまう

この攻撃の注意点(2/2)

- DNSリフレクター(DNS Amp)攻撃対策の一つであるDNS RRL(Response Rate Limiting)の導入が、この攻撃の影響を大きくする場合がある
  - DNS RRLによる応答廃棄やTCPでの再送依頼が、キャッシュDNSサーバーの負荷を高める
- キャッシュポイズニング攻撃と併用が可能である
  - 使われるDNS問い合わせのパターンが同一
    - 現在の状況は「木を隠すなら森」の状態かもしれない

2. 最近話題になっている攻撃の概要とその対策

②登録情報の不正書き換えによるドメイン名ハイジャック

このパートの構成

- DNS登録情報の流れ
- 攻撃の特徴
- 有効な対策・ポイント
- 最近の攻撃事例
- 主な事例の状況
- 「DNSハイジャック」という用語について

登録情報に対する攻撃

- ここ数年、レジストリ・レジストラの登録情報に対する攻撃事例が世界的に発生している

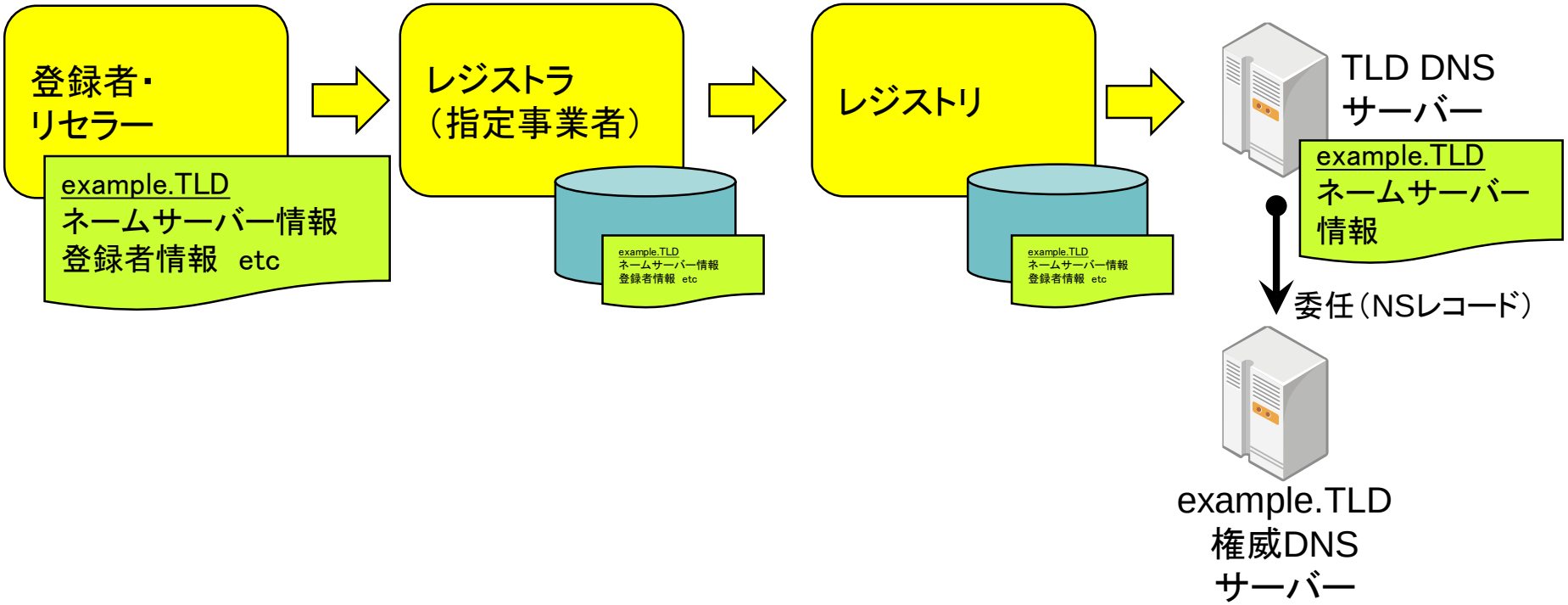
具体的には
ネームサーバー情報の
不正書き換え

```
Domain Information: [ドメイン情報]
[Domain Name]                   JPRS.JP

[登録者名]                      株式会社日本レジストリサービス
[Registrant]                    Japan Registry Services Co.,Ltd.

[Name Server]                   ns1.jprs.jp
[Name Server]                   ns2.jprs.jp
[Name Server]                   ns3.jprs.jp
[Signing Key]                   13747 8 2 (
                                DCD3F2BD0CB8A555CFC4D0866029A25C
                                4F79CEE38846DDE0A2B96AD6B6D7FD6B )
[Signing Key]                   13747 8 1 (
                                63000ECBA3DAD01FC3DFEA7DB67578DE
                                480EE0EB )

[登録年月日]                    2001/02/02
[有効期限]                      2014/02/28
[状態]                          Active
[最終更新]                      2013/03/01 01:05:07 (JST)

Contact Information: [公開連絡窓口]
[名前]                          株式会社日本レジストリサービス
[Name]                          Japan Registry Services Co.,Ltd.
[Email]                         dom-admin@jprs.co.jp
```

登録情報の例

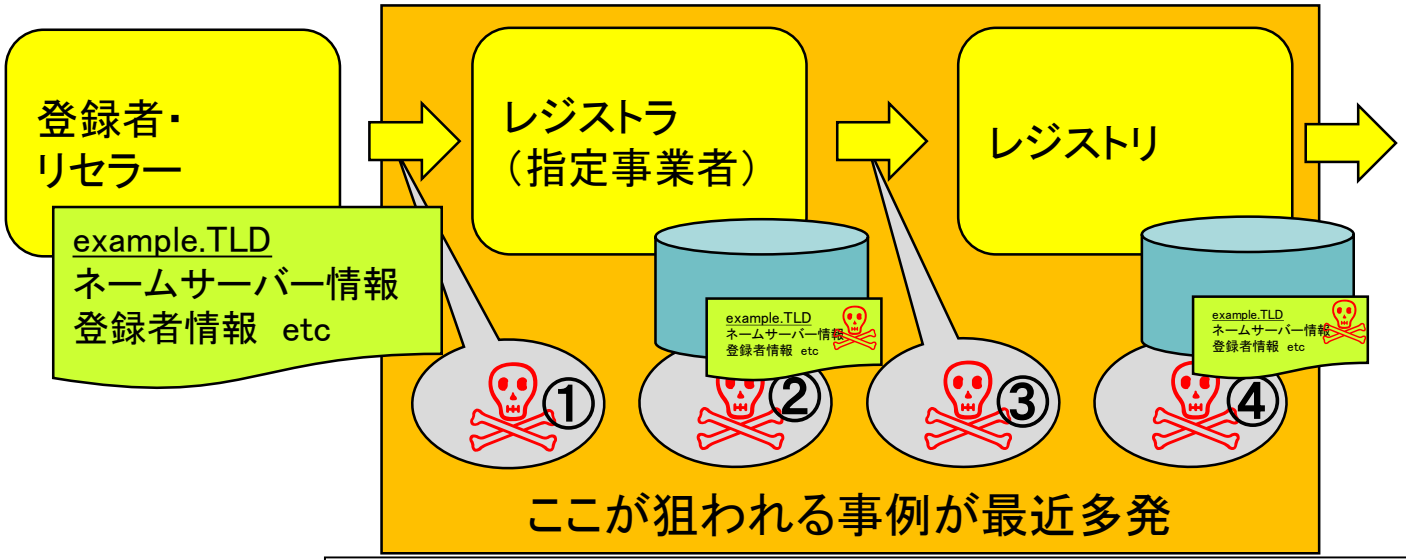
登録情報の流れ

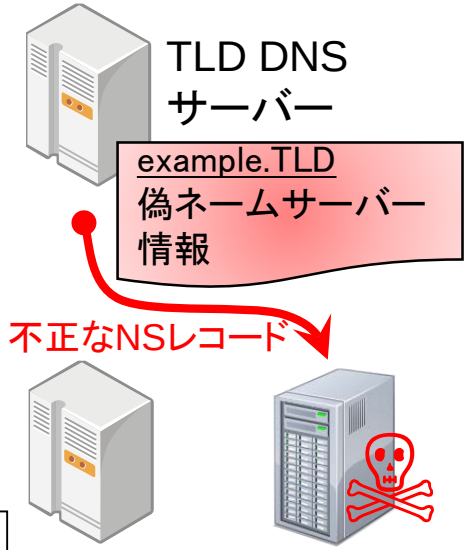
- 登録者・リセラー ⇒ レジストラ ⇒ レジストリ
- 受け取ったネームサーバー情報から、レジストリの権威DNSサーバーにNSレコードを設定



ネームサーバー情報の不正書き換え

- 流れのどこかで登録情報を不正に書き換え
- TLDの権威DNSサーバーに設定されるNSレコードを書き換え、偽の権威DNSサーバーを参照させる





例：
①登録者になりすまして、レジストラのデータベースを書き換え
②レジストラのシステムの脆弱性を突き、データベースを書き換え
③レジストラになりすまして、レジストリのデータベースを書き換え
④レジストリのシステムの脆弱性を突き、データベースを書き換え

攻撃の特徴（1/4）

- いわゆるドメイン名ハイジャックが実行される
  - 不正な登録情報によりレジストリの権威DNSサーバーのNSレコードを不正なものに書き換え、そのドメイン名へのアクセスを偽サイトに誘導
- 従来は、攻撃者による示威行為が主流であった
  - 「Hacked by 〇〇〇〇」といったページ、政治的メッセージを表示するページへの転送など
  - サイトの閲覧者などからのクレームにより状況が発覚
    - 登録情報の巻き戻しにより、数時間～1日程度で復旧

攻撃の特徴(2/4)

- 攻撃者の目的が単なる示威行為ではない場合、問題はより深刻なものとなりうる
  - ドメイン名の登録者に加え、そのWebサイトの閲覧者も攻撃の対象となりうる
  - フィッシングや情報漏えい、マルウェアの配布など
- 2014年9～10月にかけ、国内の組織が運用する複数の.comサイトにおいて当該の事例が発生
  - 攻撃者が準備した偽サイトにアクセスを誘導、特定の閲覧者に対し、マルウェアの配布を図る

攻撃の特徴(3/4)

- 著名なドメイン名が狙われやすい
  - 著名なドメイン名はアクセス数が多く、示威行為・示威行為以外のいずれにおいても標的となりうる
- 主な手口：既知の脆弱性の悪用やソーシャルエンジニアリングによるアカウントの盗難など、さまざまな手口が使われる
  - FAXによるパスワードリセットが悪用された事例もある

攻撃の特徴(4/4)

- 登録情報を扱うすべての関係者が標的となりうる
  - 登録者・リセラー・レジストラ(指定事業者)・レジストリ
- 運営基盤の弱い組織が狙われやすい
- 一度やられた組織が再度やられるケースがある
  - 根本的な脆弱性対策を実施せずサービスを再開
  - 別の脆弱性を狙われる場合もあり
- DNSSECでは防げない
  - DNSSEC関連の設定も含め、不正書き換え可能

有効な対策・ポイント（1/2）

- 基本はWebセキュリティにおける対策と同様
  - 既知の脆弱性は必ず対策しておくこと
  - ソーシャルエンジニアリングにも注意
- 著名なドメイン名の登録情報には特に注意
  - 著名な企業・団体や政府機関など
- 一部TLDでは「レジストリロック」を活用可能
  - 通常の方法での登録情報変更を禁止する仕組み
  - .jpは2015年1月19日にレジストリロックサービスを開始
    <http://jprs.jp/about/dom-rule/registry-lock/>

有効な対策・ポイント（2/2）

- チェック機構の活用
  - メールによる警告、NSレコードの設定状況の監視など
    - 「レジストラからのメールを見落としていた」という事故事例が多く観測されている
- DNSSEC関連の設定変更には要注意
  - DSレコードの削除・書き換えの監視
  - 不正書き換えの早期発見につながる可能性

最近の攻撃事例(1/2)
(2012年10月～2013年12月)

年月	対象TLDレジストリ、レジストラ
2012年10月	.ie(アイルランド)
2012年11月	.pk(パキスタン)、.ro(ルーマニア)
2012年12月	.rs(セルビア)
2013年1月	.tm(トルクメニスタン)、 .lk(スリランカ)
2013年2月	.pk(パキスタン、2回目)、 .mw(マラウイ)、.edu(gTLD)
2013年3月	.bi(ブルンジ)、.gd(グレナダ)、 .tc(英領タークス・カイコス諸島)、 .vc(セントビンセントおよび グレナディーン諸島)
2013年4月	.kg(キルギスタン)、.ke(ケニア)、 .ug(ウガンダ)、.ba(ボスニア)、 .om(オマーン)、.mr(モーリタニア)

注:JPRSにおいて把握しているもののみ

年月	対象TLDレジストリ、レジストラ
2013年5月	.mw(マラウイ、2回目)
2013年7月	.my(マレーシア)、 .nl(オランダ)、 .be(ベルギー、同一月内に2回、 登録情報には被害なし)、 Network Solutions(gTLDレジストラ、 登録情報には被害なし)
2013年8月	.nl(オランダ、2回目)、 .ps(パレスチナ)、 Melbourne IT(gTLDレジストラ)
2013年9月	.bi(ブルンジ、2回目)、 .ke(ケニア、2回目)
2013年10月	Network Solutions(gTLDレジストラ)、 Register.com(gTLDレジストラ)、 .my(マレーシア、2回目)、 .cr(コスタリカ)、.qa(カタール)、 .rw(ルワンダ)

最近の攻撃事例(2/2)
(2014年1月～2015年1月)

年月	対象TLDレジストリ、レジストラ
2014年1月	.me(モンテネグロ)
2014年2月	MarkMonitor(gTLDレジストラ、登録情報には被害なし)、 .uk(英国)
2014年9月～10月	Network Solutions(nikkei.com)、 eNom(st-hatena.com)(注2)
2014年10月	.id(インドネシア)、 .qa(カタール、2回目)
2014年11月	Network Solutions(craigslist.org)、 GoDaddy(gigya.com)
2014年12月	.ca(カナダ)
2015年1月	WebNIC(malaysiaairlines.com)

注1:JPRSにおいて把握しているもののみ

注2:国内の組織が運用する複数の.comドメイン名において事例発生を確認した旨の情報あり、状況調査中

主な事例の状況（1/8）

- .tm、.lk（2013年1月）
  - 登録者の電子メールアドレスと平文パスワードが流出
    - .tm：約5万件、うち.jpのメールアドレス約1000件
    - .lk：約1万件
  - 原因：登録画面のSQLインジェクション脆弱性
- .edu（2013年2月）、.nl（2013年7月）
  - 全登録者・レジストラのパスワードの強制リセット
  - パスワードファイルの外部流出が疑われたため
    - 同年1月末のmit.eduのドメイン名ハイジャック事例との関連性
    - 同年8月の.nlの事例（後述）との関連性

主な事例の状況（2/8）

- .nl（2013年8月）
  - あるレジストラのパスワードがクラック
    - レジストラが管理するドメイン名数千件がハイジャックの被害に
  - マルウェア配布サイトに誘導
    - ドライブ＝バイ＝ダウンロードの手法を利用
      （当該Webページを開いただけでマルウェアを強制ダウンロード）
  - 前回（2013年7月）の事件で流出したID/ハッシュパスワードがクラックに使われた可能性あり（未確認）
    - 流出したパスワードは.nlレジストリ（SIDN）により強制変更済
    - パスワードを元に戻したレジストラがあった可能性

主な事例の状況（3/8）

- Melbourne IT（2013年8月）
  - 「シリア電子軍」を名乗る者による犯行
  - あるリセラーのアカウント情報を盗まれ、リセラーの登録システムに不正侵入
  - リセラーの登録システムに存在した脆弱性を突き、本来は書き換えることのできない、別アカウントが管理するドメイン名登録情報を不正書き換え
    - nytimes.com、twimg.comなどがドメイン名ハイジャックの被害に
  - 不正書き換えされたNSレコードのTTLが長かったため、DNSキャッシュが長時間にわたって残存し、影響が長時間に及んだ

主な事例の状況（4/8）

- Network Solutions、Register.com（2013年10月）
  - パレスチナに関する政治的声明が書かれたWebページにアクセスを誘導
  - アンチウイルスベンダー・著名なWebサービス・セキュリティベンダーなどが被害に
    - avira.com, avg.com
    - alexa.com, leaseweb.com, redtube.com, whatsapp.com
    - metasploit.com, rapid7.com
  - レジストラへのFAXによりメールアドレス設定・パスワードをリセットする手口が使われた
    - レジストラのサービスを悪用

主な事例の状況（5/8）

- MarkMonitor（2014年2月）
  - 「シリア電子軍」を名乗る者による犯行
  - レジストリロックが効果を発揮
    - facebook.com、paypal.com、ebay.com、google.com などは被害を免れた
    - 当時レジストリロックを実装していなかった.uk（paypal.co.uk、ebay.co.uk）は、被害を受けた
  - .ukでは2014年3月にレジストリロックを実装

主な事例の状況（6/8）

- Network Solutions、eNom（2014年9~10月）
  - 国内の組織が運用する複数の.comサイトが標的に
    - nikkei.com
    - st-hatena.com
  - 単なる示威行為ではなく、Webサイトの閲覧者をも直接の攻撃対象としている
    - 特定の閲覧者に対し、マルウェアの配布を図る
  - 不正書き換えの隠蔽を図っている
    - ネームサーバー情報の全部ではなく一部のみを書き換え
    - 1～2日程度で元の登録情報に巻き戻し
  - 具体的な攻撃手法・原因などについては現在も調査中

主な事例の状況（7/8）

- GoDaddy（2014年11月）
  - 「シリア電子軍」を名乗る者による犯行
  - 顧客サービス用のWebサイトが標的に
    - 正規の登録者に成りすましてGoDaddyに不正ログイン
    - 「gigya.com」のNSが書き換えられ、Gigya社の顧客サイトから読み込まれるコンテンツが置かれる「cdn.gigya.com」サイトが、別サイトにすり替えられた
    - その結果、多数のサイトが被害に遭った
      - 毎日新聞、so-netなど国内の複数のサイトにも被害あり

主な事例の状況（8/8）

- .ca（2014年12月）
  - オンタリオ州政府のドメイン名が標的に
    - ontario.ca、gov.on.ca
  - レジストラ（EasyDNS）の声明によると、正規の登録者に成りすまして不正ログインしたとのこと

「DNSハイジャック」という用語について

- 「DNSハイジャック」は登録情報の不正書き換え以外に、下記の例なども含めたDNS対応付けの書き換え行為全般を示す用語としても使われている
  - 利用者が使うキャッシュDNSサーバーの不正変更
  - ISPのキャッシュDNSサーバーにおけるフィルタリング
  - 参考：Wikipedia英語版：DNS hijacking
    <http://en.wikipedia.org/wiki/DNS_hijacking>
- そのため、攻撃の内容やその対策を具体的に示したい場合、適切な用語ではない

JPRSではこうした事例について「登録情報の不正書き換えによるドメイン名ハイジャック」という用語を使用

Comments & Questions