補足資料：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その対策について

初版作成：2014年11月5日

株式会社日本レジストリサービス（JPRS）

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

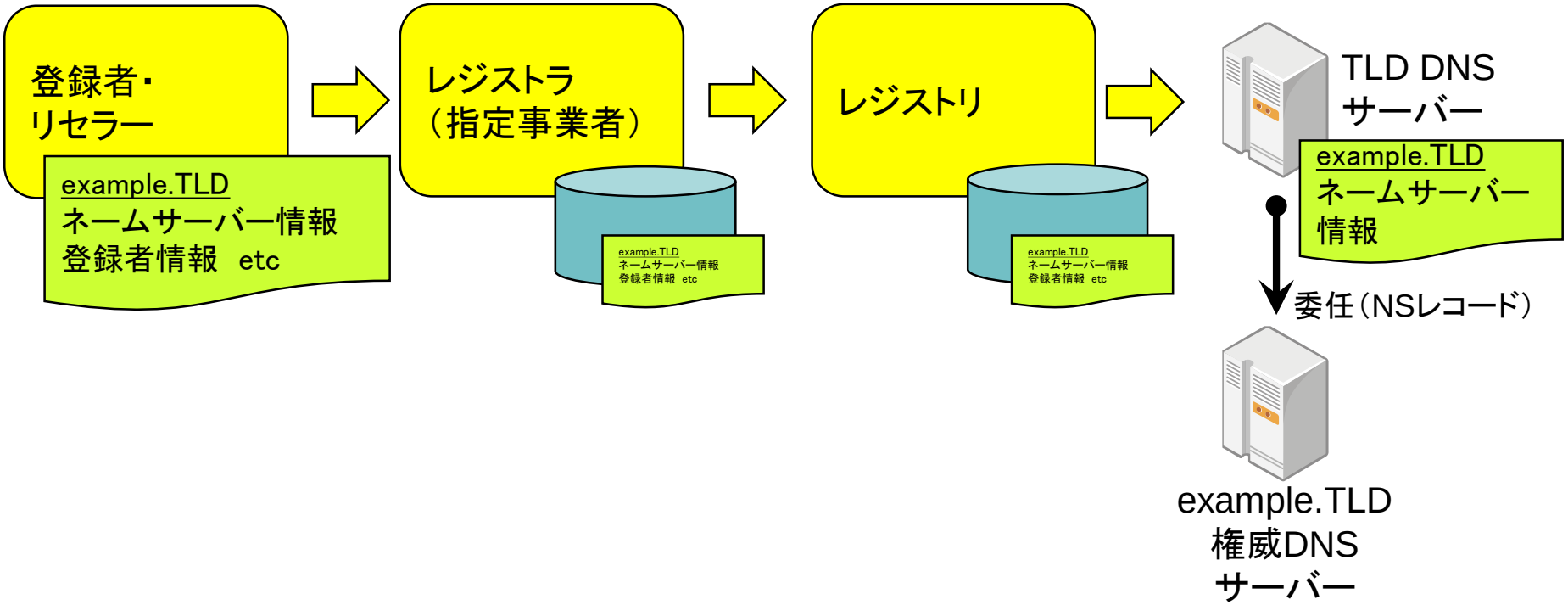
具体的には
ネームサーバー情報の
不正書き換え

```
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

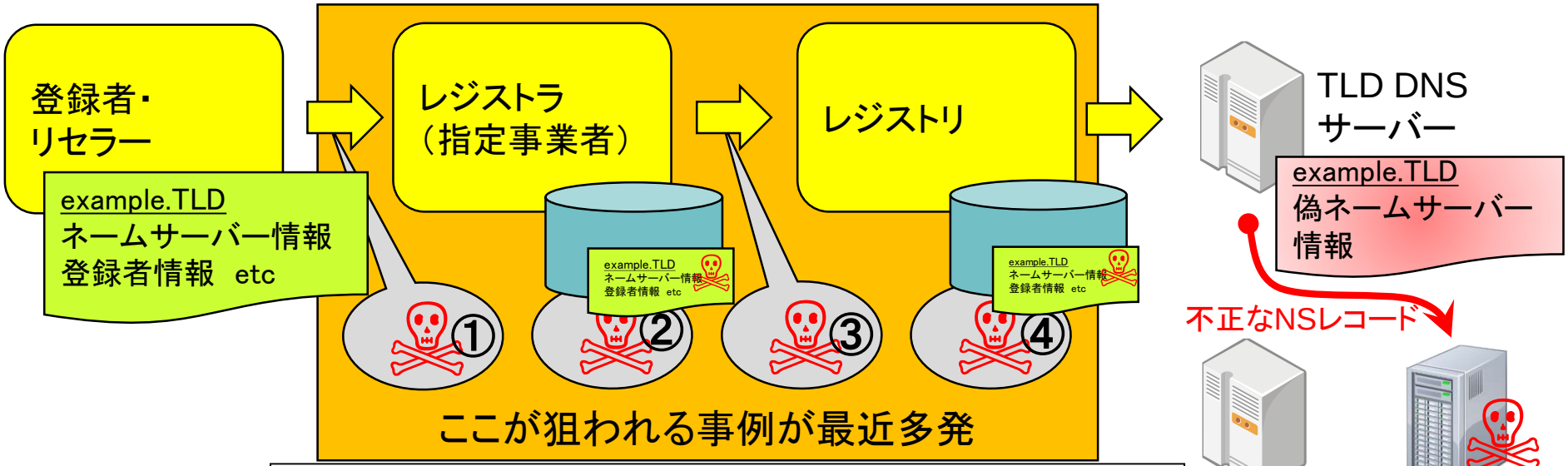
登録情報の流れ

- 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

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

付録1：レジストリ・レジストラが攻撃されたこれまでの事例とその状況

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～10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	.com(gTLD、注2)
2014年10月	.id(インドネシア)、 .qa(カタール、2回目)

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（1/6）

- .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（2/6）

- .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（3/6）

- 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（4/6）

- 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（5/6）

- 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（6/6）

- .com（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
  - 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調査中

付録2：用語「DNSハイジャック」について

用語：「DNSハイジャック」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では今回の事例について「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