2013年12月25日
第47回JPドメイン名諮問委員会
資料３

レジストリ･レジストラへの攻撃について

2013年12月25日（水）
株式会社日本レジストリサービス

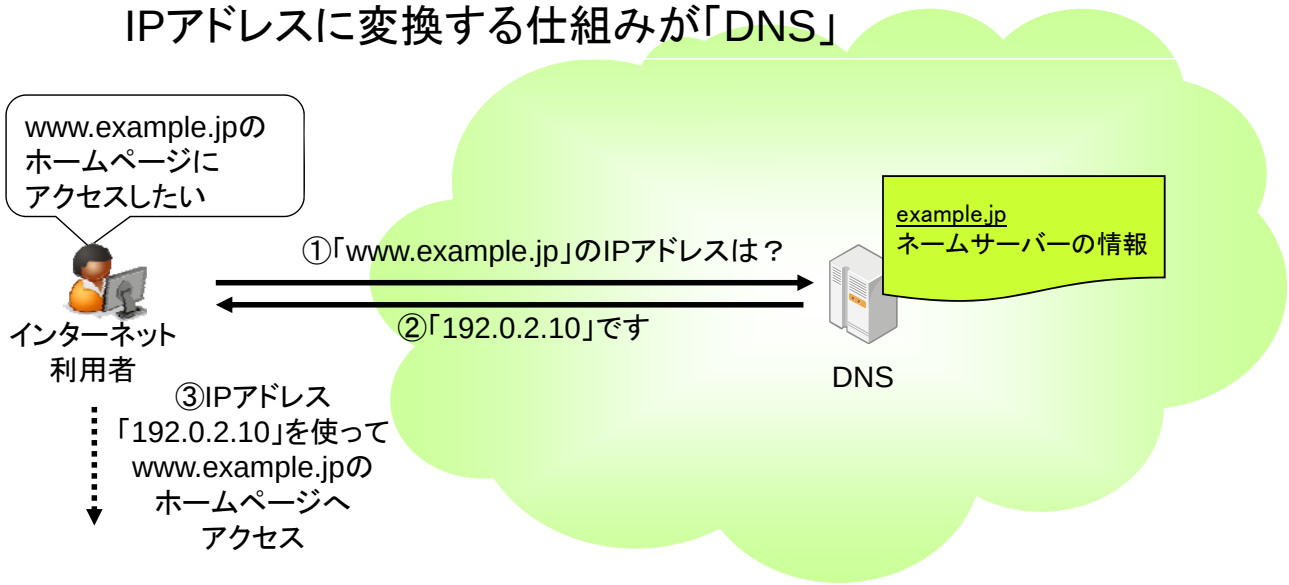
概要

- 最近、レジストリやレジストラが管理するドメイン名の登録情報に含まれるネームサーバー情報を不正に書き換える事例が、数多く発生している
- この登録情報はDNS（後述）に登録されている
- 登録情報の例
  - 登録者名
  - 公開連絡窓口
  - ネームサーバー
  - 署名鍵（DNSSEC）

```
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
```

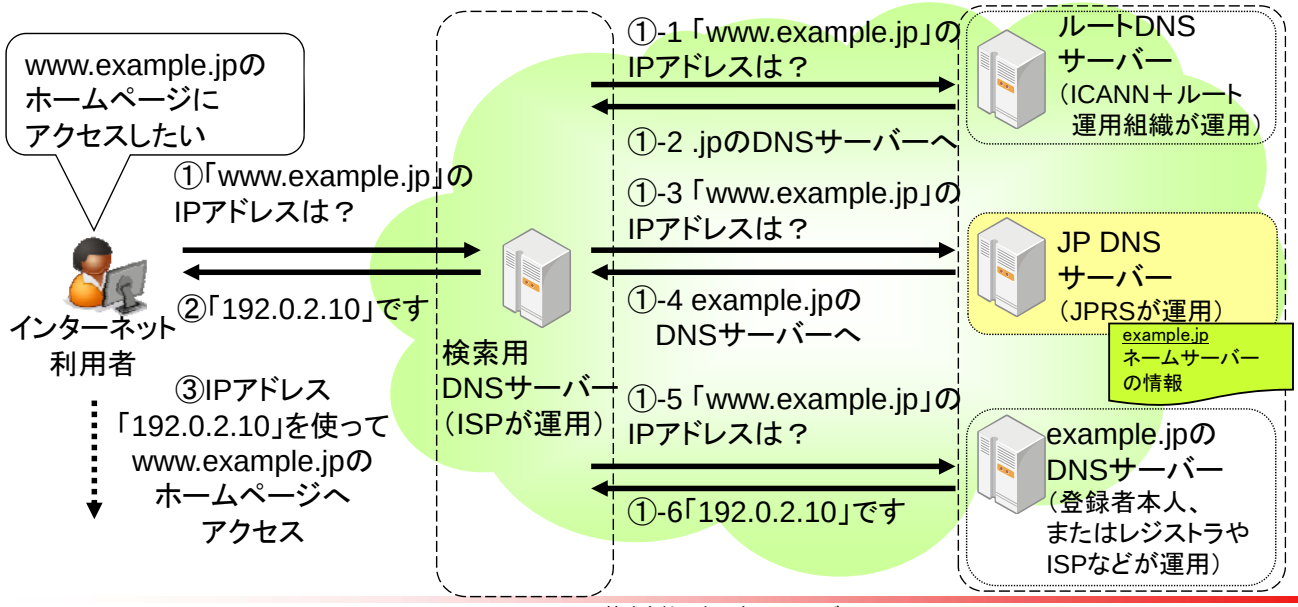
DNS:ドメイン名を利用するための仕組み

- インターネットでの通信はIPアドレスを利用
- ドメイン名をインターネット上で利用するために、対応するIPアドレスに変換する仕組みが「DNS」



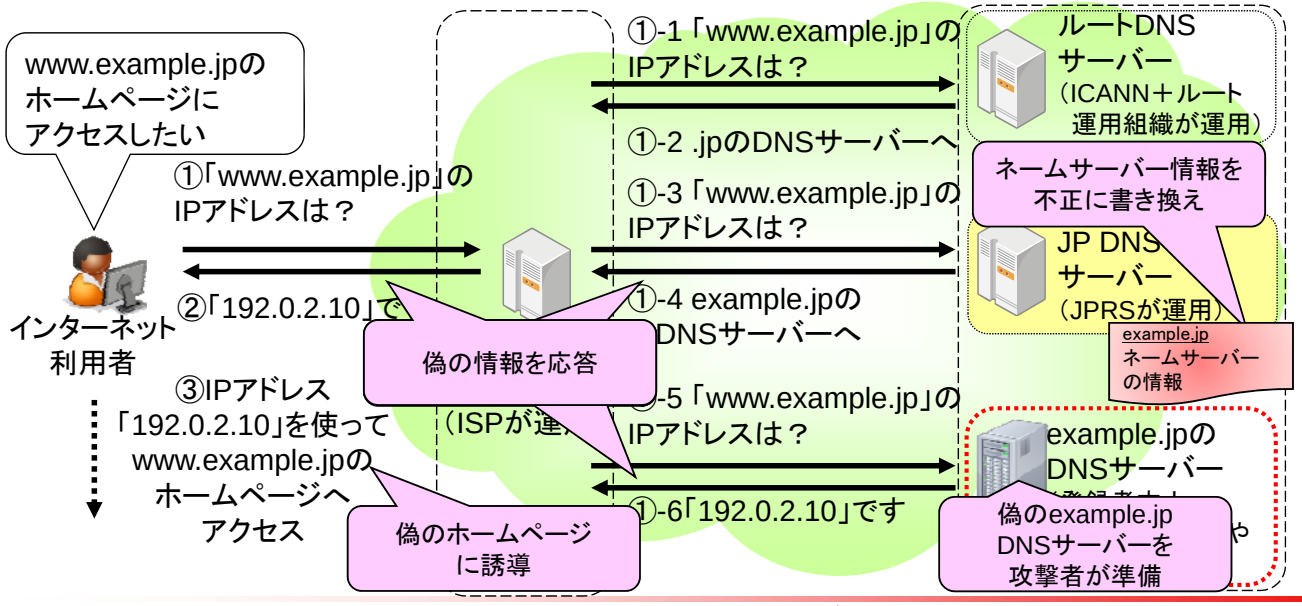
DNS:2種類のサーバー

- 2種類のDNSサーバー
  - 情報を検索するためのDNSサーバー群（キャッシュDNS）
  - 情報を公開するためのDNSサーバー群（権威DNS）
- 多数のDNSサーバーが連携して動作



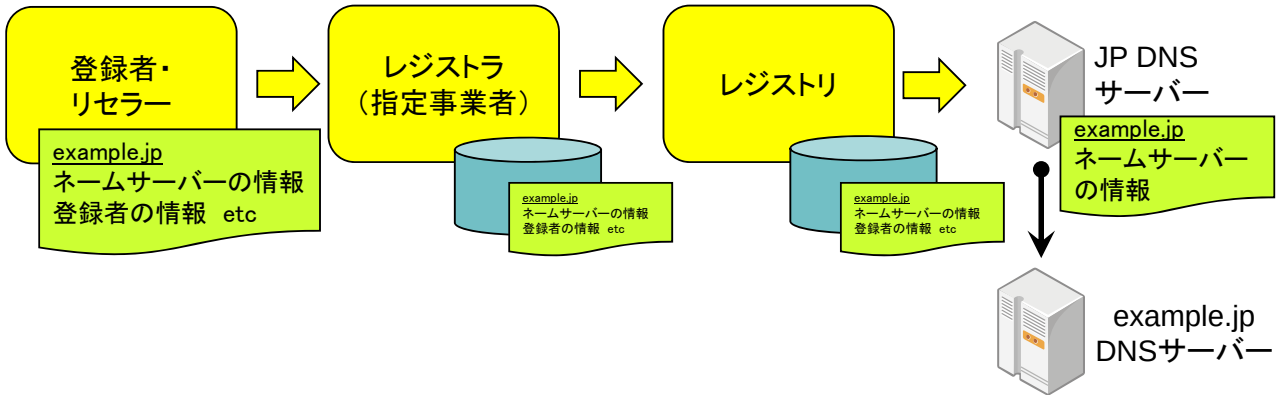
ドメイン名ハイジャック

- 登録情報に含まれるネームサーバー情報を不正に書き換え、偽のホームページに誘導



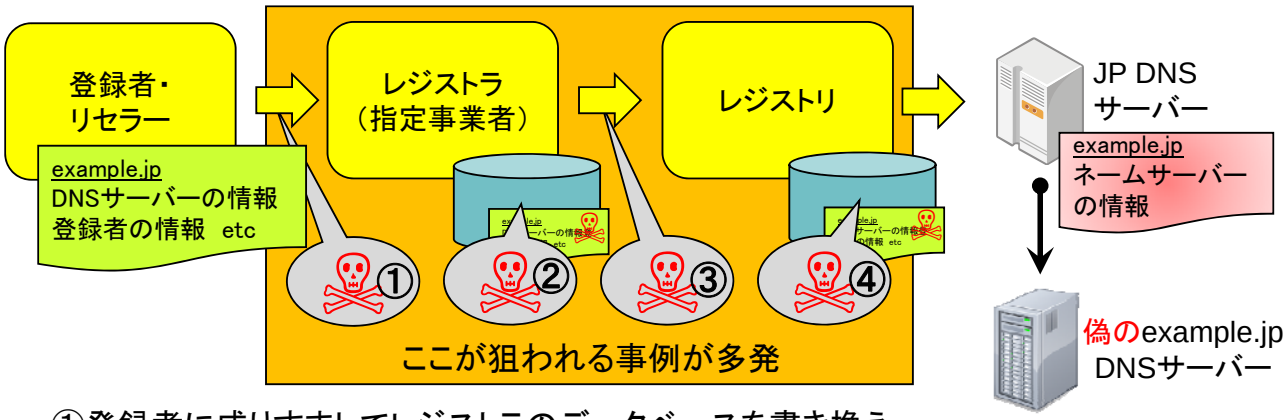
登録情報の流れ

- 登録者（リセラー）⇒レジストラ⇒レジストリ
- レジストリは登録情報をもとに権威DNSを設定



登録情報の不正な書き換え

- 流れのどこかで登録情報を不正に書き換え
- レジストリ・レジストラが狙われる事例が多発



①登録者に成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に不正侵入し、レジストラのデータベースを書き換え
③レジストラに成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に不正侵入し、レジストリのデータベースを書き換え

最近の発生事例（時系列順）

年月	TLDレジストリ、レジストラ/リセラー
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)

年月	TLDレジストリ、レジストラ/リセラー
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、登録情報の書き換えはなし)、 Network Solutions(gTLDレジストラ、登録情報の書き換えはなし)
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)

注1 JPRSが把握しているもののみ

※外部に公開されている情報をJPRSが調べたものであり、内容の正確性は保証できません。

攻撃の原因と動機

- 既知の脆弱性を悪用する事例が多い
  - サーバーのソフトウェアの脆弱性
  - Webサイトの脆弱性
- これまでのところ、攻撃者の示威行為や政治的メッセージの発信にとどまっている

JPRSの主な取り組み

- 脆弱性情報の収集と対応
- システムの脆弱性試験
- 指定事業者に認証情報管理の徹底を注意喚起
- 成りすましの事実が判明した指定事業者アカウントの緊急停止
- レジストリロックの導入検討
  - レジストリロックされたドメイン名は、あらかじめ決められた登録者（の特定の所属員）のみが登録情報を変更でき、レジストラによる登録情報の変更はできない
  - 登録情報の変更において、登録者への直接の意思確認が行われる