「ドメイン名ハイジャック」及び「DNSポイズニング」の危険性に関する一連の注意喚起について

＋緊急対策のお願い

2012年7月4日

日本レジストリサービス（JPRS）

本件に関する2件の注意喚起

- 2012年6月22日公開

  「サービス運用上の問題に起因するドメイン名ハイジャックの危険性について」

  http://jprs.jp/tech/security/2012-06-22-shared-authoritative-dns-server.html

- 2012年7月4日公開

  「権威／キャッシュDNSサーバーの兼用によるDNSポイズニングの危険性について」

  http://jprs.jp/tech/security/2012-07-04-risk-of-auth-and-recurse.html

どんな危険性があるのか？（ドメイン名ハイジャック）

- サービス事業者が顧客に提供するDNSサービス／システムにおいて、
  - 複数の顧客のドメイン名（ゾーン）を、同一の権威DNSサーバーに共存させる形で運用している
  - かつ、顧客によるゾーンの新規作成を許可している
  - かつ、サービス事業者のシステムにおいて、顧客が作成するゾーンの内容のチェック・制限が不十分である

  …場合、悪意を持つ第三者に顧客のドメイン名をハイジャックされる危険性がある

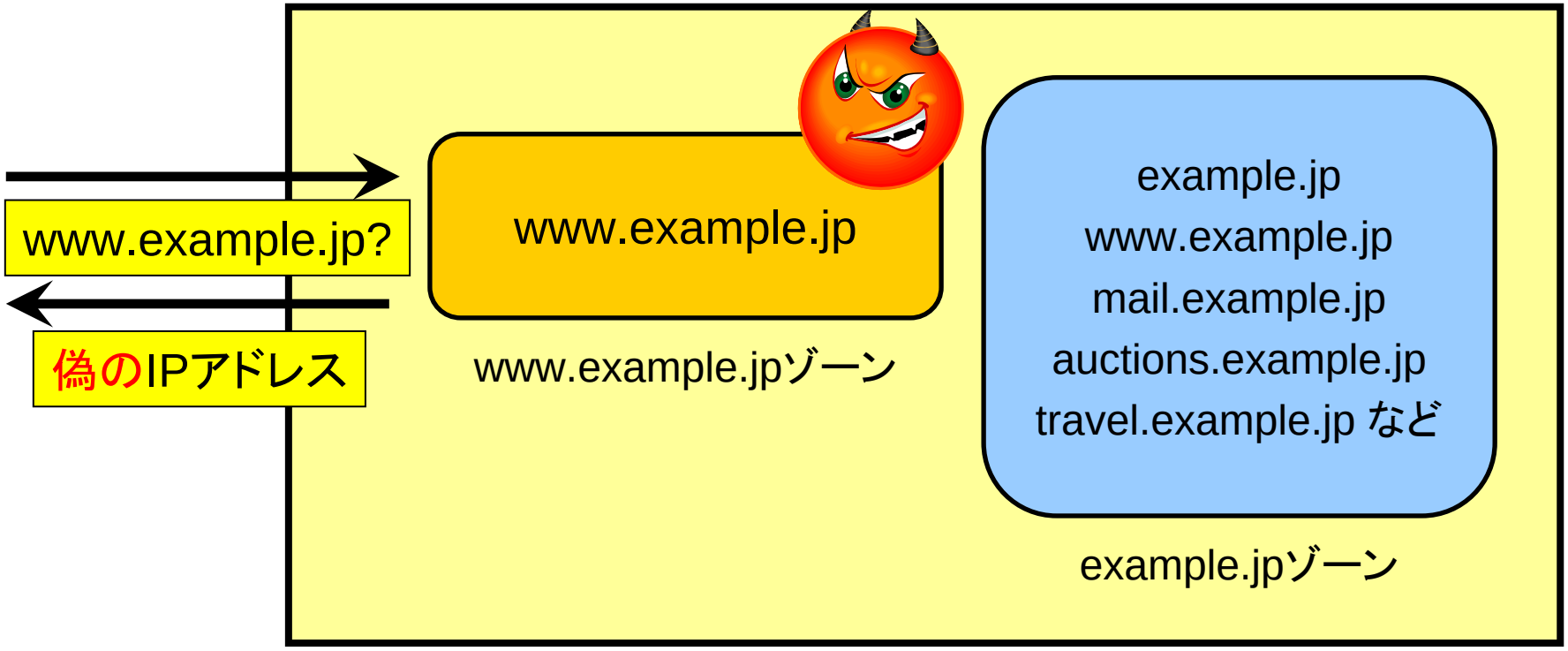
どんな危険性があるのか？（DNSポイズニング、引っ越しの妨げ）

- さらに、当該の権威DNSサーバーがキャッシュDNSサーバーを兼用していた場合、危険性はさらに深刻となる
  - 任意の名前に対するDNSポイズニングの危険性
  - ドメイン名の引っ越しが妨げられる危険性

ドメイン名ハイジャックとは？

- ドメイン名の権限を持たない第三者が、不正な手段でドメイン名を自分の支配下に置くこと
- ドメイン名ハイジャックの方法例
  ① レジストリの登録情報を不正に書き換える
  ② 権威DNSサーバーに不正なデータを登録する
  ③ キャッシュDNSサーバーに不正なデータをキャッシュさせる
- 今回のものは「② 権威DNSサーバーに不正なデータを登録する」手法を使用

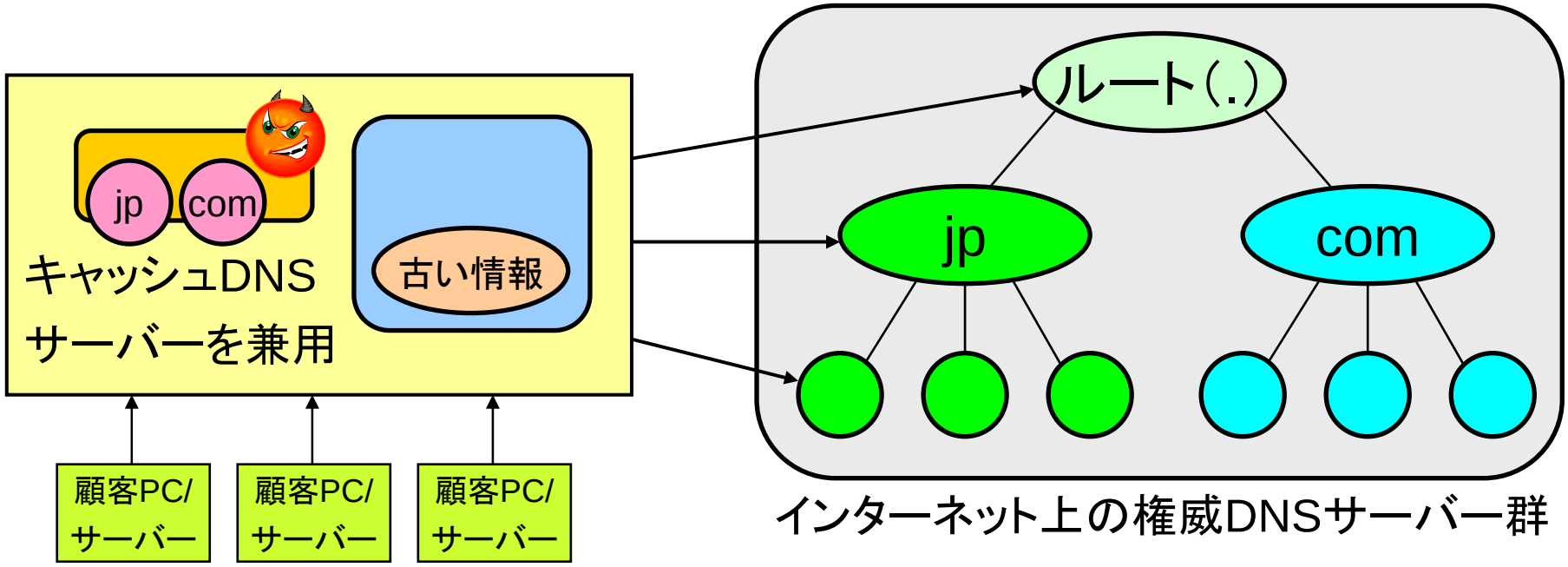
今回のドメイン名ハイジャックのしくみ



サービス事業者が運営する権威DNSサーバー

- 顧客が運用中のドメイン名のサブドメインを同一サーバー内に作成
- 現在の多くのDNS実装では、より階層の深いゾーンのデータのみが使われる
- 上記の例では「*.example.jp」のすべての名前がハイジャック可能
  - つまり、単なる「サブドメインハイジャック」ではない！

キャッシュDNSサーバーを兼用していた場合、問題はさらに深刻



- 任意の名前に対するDNSポイズニングが可能になる
  - キャッシュポイズニングと同様の攻撃をより確実に実行できる
  - 攻撃者にjpやcomを作成された場合、その下のすべての名前を奪われる
- 退会後も古い情報が残っていた場合、ドメイン名の引っ越しが妨げられる

サービス事業者のみなさまへ（ご確認と緊急対策のお願い）

- 以下の点について、早急なご確認をお願いいたします
  - 貴社のサービス／システムにおいて、運用中のドメイン名のサブドメインや上位ドメインを、別顧客が作成可能になっていないか？
  - 顧客のドメイン名を収容する権威DNSサーバーと、顧客PC/サーバー向けキャッシュDNSサーバーを兼用していないか？
- もし該当する場合、早急に以下の緊急対策をよろしくお願いいたします
  - 運用中のサブドメイン／上位ドメインの、別顧客による作成の制限（少なくとも、自動的な登録の禁止）
  - 当該権威DNSサーバーとキャッシュDNSサーバーの分離