不適切なドメイン名管理が招く脅威

2005年12月6日

株式会社日本レジストリサービス(JPRS)

http://米谷嘉朗.jp/

不適切なドメイン名管理とは

- ドメイン名登録者が管理すること
  - ゾーン情報を提供するDNSサーバの運用(下位)
  - そのDNSサーバ情報のレジストリへの設定(上位)
  - 下位と上位の整合性維持

いずれが欠けても「不適切」な管理状態

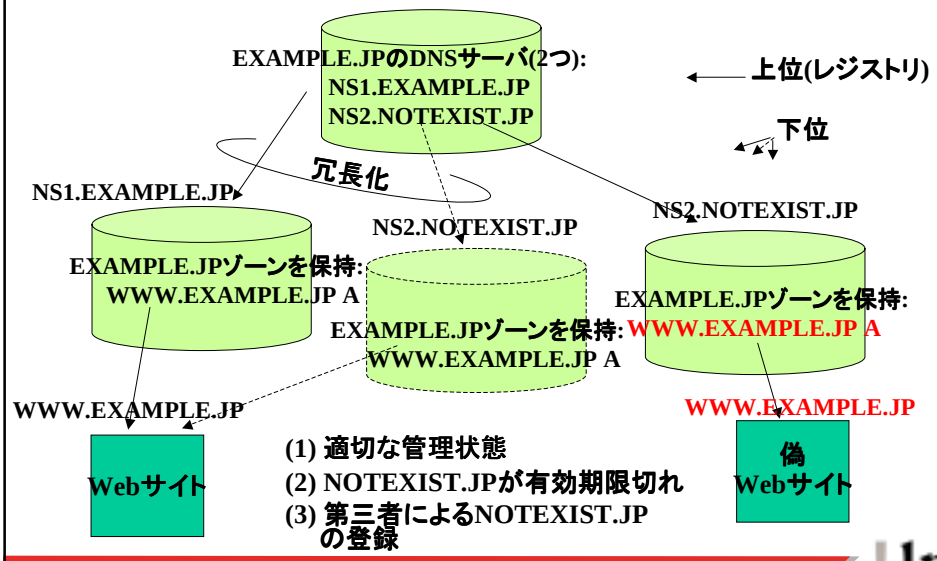
- 不適切なドメイン名管理の原因
  - レジストリに間違った情報を登録してしまっている
    - DNSサーバ名やIPアドレスの書き間違いなど
  - 有効期限切れ(存在しない)ドメイン名のネームサーバを上位に残してしまっている
  - 機能していないDNSサーバ(下位)を上位に残してしまっている

不適切な管理状態には「ドメイン名の乗っ取り」の脅威が内在する

ドメイン名の乗っ取りはなぜ起きるのか

- ゾーン情報を提供するDNSサーバのドメイン名が有効期限切れの場合を想定
  - EXAMPLE.JPはNS1.EXAMPLE.JPとNS2.NOTEXIST.JPをDNSサーバとして上位に設定（ex.1年前）
  - NOTEXIST.JPは有効期限が切れ、存在しなくなった（ex.2ヶ月前から）
  - 誰もがNOTEXIST.JPを登録でき、かつ、EXAMPLE.JPのゾーンを提供するDNSサーバとしてNS2.NOTEXIST.JPを立ち上げることができる（ex.今この瞬間）
  - 立ち上げた人は、NS1.EXAMPLE.JPと異なる応答を返す偽のゾーンを運用可能となる（ex.すぐ後）
- この状況は容易に起こり得る
  - ドメイン名登録管理者とDNS運用管理者間が別組織で、両者間の連携が取れていない場合など

ドメイン名乗っ取りの例(イメージ)



ドメイン名が乗っ取られると何が起きるか

1. DNSサーバが応答を返さない
   - 名前解決に遅延が生じる
2. DNSサーバが問合せドメイン名は存在しないと応答する
   - アクセスできるはずのドメイン名にアクセスできなくなる
3. DNSサーバが問合せドメイン名に対して不正な情報を応答する
   - 偽Webサイトに誘導する
   - メールを不正中継して盗聴・改ざんする

ドメイン名登録者の信用・信頼が失墜する

実際の事例

- あるクレジットカード会社のドメイン名はDNSサーバを2つ設定していた
- そのうち1つのDNSサーバはドメイン名が有効期限切れとなり、誰もが登録できる状態となった
- その状態に気づいた人が、期限切れとなったドメイン名を登録して脅威を回避した上で、IPAなどに報告を行った
- その脅威について、2005年6月27日にIPAが注意喚起を行った
  - それに引き続き、JPCERT/CC、総務省、JPRSも注意喚起
  - 各種Webメディアでも取り上げられた

誰の責任?

- ***ドメイン名の管理はドメイン名登録者の責任***
  - ドメイン名登録情報の正確性の確認、維持はドメイン名登録者が実施すること
  - レジストリは単にドメイン名登録者や指定事業者からの申請に基づいてゾーン情報を更新している
- 一方、レジストリや指定事業者は不適切な管理状態を把握可能
  - レジストリができること
    - 啓発・教育
    - 状態の確認と個別通知

JPでの対応

- Webサイトでの注意喚起
- JPドメイン名での不適切な管理状況の確認
  - DNSサーバ名がJPドメイン名でない場合は確認の対象外
- 注意喚起メールの送付
  - ドメイン名登録者、ドメイン名登録指定事業者
    - 電子メール、郵政メール
  - 2005年8月、9月、10月の3ヶ月(3回)実施
- 国内外のコミュニティで報告・注意喚起
  - CENTR、ICANN、IEPG、セキュリティセミナー、DNS Day
- 存在しないJPドメイン名のDNSサーバへの委任削除実施
  - JPドメイン名の規則(技術細則)を改訂(2005年12月5日公表、2006年1月10日実施)
  - 存在しないJPドメイン名のDNSサーバへの委任を定期的に確認・削除

参考URI

- DNSの健全な運用のために
  - http://jprs.jp/tech/dnsqc/index.html
- DNSサーバの不適切な管理による危険性解消のための取り組みについて
  - http://jprs.jp/info/notice/problematic_ns.html
- ドメイン名の登録と DNS サーバの設定に関する注意喚起
  - http://www.ipa.go.jp/security/vuln/20050627_dns.html
- ドメイン名の運用管理に関する注意喚起
  - http://www.soumu.go.jp/joho_tsusin/domain/050630.html