
# ざっくりわかる インターネットプログラミング

ダイアモンドアプリコット電話研究所
**山崎 はるか**
YAMAZAKI, Haruka
*http://www.nda.co.jp/*

## 第9回 ドメイン情報にふれる ～Whoisクライアント

### なりすまし

WebページやSQL Serverへのアクセス制限を「ドメイン名」で振り分けている人がいるが、あれは危険だ。ドメイン名は、DNSを使えばカンタンになりすませるからだ。

たとえば、「tokyo033.ppp.ybb.ne.jp」というドメインからのみ、あなたのSQL Serverに接続できるように設定していたとする。

するとSQL Serverは、アクセスされるたびに、DNSにIPの逆引き（名前解決）を行ない、アクセスしてきたIPが、許可されたドメインに合致しているか確かめる。

この方法なら、アクセス権者のIPが（引越しなどで）変わってもドメインが合致していれば引き続き認証できるし、また、グループ（会社）単位での認証もカンタンに行なえるだろう。

しかし、ハッカーが、自身のIPを自身のDNSに「tokyo033.ppp.ybb.ne.jp」と設定して、アクセスしてきたらどうだろう（逆引き時の返答ドメイン名は、誰でも好き放題に名乗れる）。

そんなときも、あなたのSQL Serverは、通常の逆引きと同じく、最終的にハッカーのDNSに問い合わせて名前解決することになる。その結果、まったく知らないIPを「tokyo033.ppp.ybb.ne.jp」と誤認して、通してしまうことになる。

これが ドメインのなりすまし、いわゆるスプーフィング（詐称）である(図1)。

ドメイン名単位のアクセス制限は、

・無線LAN保守用ページ
・掲示板の管理用Auth

などでよく見られる。

とくに管理者のメールヘッダーには、日ごろ、よく使っているIP／ドメインが書かれていることが多いから、このドメインを自身のDNSに転記し、ターゲットにアクセスを行なうことで、容易に突破できることがある。これを防ぐには、

・外部アクセス制限はなるべくIP単位（可能ならMACアドレス単位）で行

**Level**
1 2 3 4 5

**Technology Tools**
- [x] Visual Basic
- [ ] Visual C#
- [ ] Visual C++
- [ ] SQL Server
- [ ] Oracle
- [ ] Access
- [ ] ASP.NET
- [ ] Other:

**Samples**
この記事で取り上げたソースコードおよびサンプルプログラムは、
http://www.shoeisha.com/mag/windev/
からダウンロード可能です。

図1：ドメイン名で認証すると容易になりすまされる

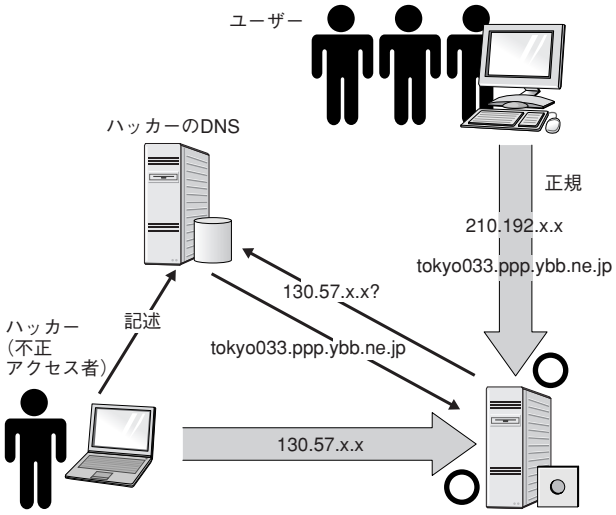


図2：whoisはUNIXの標準コマンドのひとつ


なう

・不正なアクセスとおぼしき記録が出たときは必ずIPの“所在”を確認し、場合によっては、そのIPもろともフィルタレベルで閉じる（全閉塞させる）

という作業が必要となる。

そしてこれらの確認作業を正しく行なうときに、非常に便利なのがwhois（NICNAME）なのである。

## 速習！ whois

whois（フーイズ）は、UNIXの標準コマンドのひとつである（図2）。

このコマンドはWindowsのプロンプトにはないので、「Whois Gateway」のようなWebサービスをイメージする人も多いかもしれない。

しかし元々のwhoisは、レジストラ団体が管理する「Whoisデータベース」に接続するためのプロトコルのことである。

考察してみよう。

独自ドメインを申請するときは、レジストラ団体（日本ではJPRSなど）に名前や住所／電話番号を申請（記入）しなければならない。

Whoisデータベースはこの一部分である。

レジスト“リ”団体（日本ではJPNIC）はこの情報にはほとんど関わっていない。あくまでネームサーバーの管理である。

これらの関係は、図3のようになっている。

これらのデータベースが公開されるのは、

「（ドメイン統括者は）調停者であり、管理者であり、技術者であらねばならない」

（RFC1033ドメインアドミニストレーターガイド）

というポリシーが基盤にある。

図3：登録情報の流れ（JPドメインの場合）