インターネットのセキュリティに対する正しい認識

鈴木常彦
Tsunehiko Suzuki, 中京大学情報理工学部 (豊田市貝津町床立 101, tss@sist.chukyo-u.ac.jp)

要約
インターネットが何であるか定義できるだろうか。インターネットに安全，安心を求めてはいけない。今日のインターネット社会は砂上の楼閣である。本論ではインターネットがいかに信用できないものであるかを，その基盤であるDNSとルーティングを中心に解説するとともに，セキュリティ対策として必要なことは，技術よりも参加者すべての自覚に基づく自律と協調であることを論ずる。

キーワード
Internet, spam , DNS, 経路ハイジャック , integrity, 電子証明書

インターネットとは

インターネットにおけるセキュリティを考察してみよう。それにはまず，そもそもインターネットとは何なのかをしばし考えてみる必要がある。たとえば，学校をインターネットに接続するということはどういうことなのだろうか。インターネットサービスプロバイダ（以下プロバイダ）とは何をサービスしてくれるものなのか。プロバイダの約款を読んでみてもらいたい。世界と接続させてあげるとは書いてないはずである。プロバイダはプロバイダとあなたの学校との接続を提供しているにすぎない。場合によっては近所の局までの接続しか約束されていないこともある。

インターネットとはインターネットに接続していると思っている人たちの共同幻想である。インターネットに接続するということは共同幻想に参加することである。しかし，あなたの思っている幻想と私の思っている幻想は違うものかもしれない。何がどうなっているとインターネットであって，何が失われるとインターネットでなくなるのか。深い考察が必要である。

プロバイダとは自分の商品であるインターネットが何であるかにできるだけ触れられないよう，そっと，そして血の滲むような努力によって，その幻想を守り続けようとする組織なのである。

幻想としてのDNS

セキュリティのすべての基礎はIntegrity，すなわち真正性（あるいは完全性）である。あなたが通信しようとするとき，その相手はあなたが思っている相手でなくてはならない。

インターネット幻想の構成要素にドメイン名とDNSがある。サーバに名前を付けることができると大変便利であることはいうまでもない。しかし，世界中に同じ名前のサーバが乱立したのでは混乱が生ずる。つまり，真正性が担保できなくなる。

そこで「ひとつのインターネット(The Internet)」という幻想を共有したい人々はひとつの合意を行うことになる。DNSという名前管理システムを共用するため，共通のルートサーバを信用しようという合意である。多くの人々はICANN[*1]という組織が管理するルートサーバを信じ，またDNSという仕組みがその名前空間の真正性を担保してくれると信じて，ひとつの共同幻想に参加をしているのである。

しかしこの幻想はあまりに脆い。DNSというシステムの真正性はあまりに容易にやぶられる。真正性に対する幻想が守られるためには以下のような前提が最低限必要になる。

1. あなたの使うパソコンに設定されたDNS検索サーバ（正しくはフルリゾルバあるいはDNSキャッシュサーバ）があなたの信じているものであること

2. あなたの信じているDNS検索サーバに，

あなたの信じているルートサーバが正しく設定されていること

3. ルートサーバのデータが正しいこと

4. あなたの検索したいトップレベルドメイン (JP とかCOM等，以下TLD ）のDNS サーバが正しく運用されていること

5. あなたの検索したいドメインのDNS サーバ（正しくはDNS 権威サーバ）が正しく運用されていること

6. あなたのDNS 検索サーバが受け取っている世界のDNS サーバたちからの応答が，本物の相手からの応答であること

7. 真正性を共有したいあなたの友人も同じ前提に立っていること

これらの前提を守るのは非常に困難であるどころか，個々の努力だけではどうにもならないと言って良い。

ともあれ順に確認すべき事項をみていこう。

1. DNS 検索サーバは本物か

DHCP で自動設定している場合， DHCP サーバ自体が悪意ある偽物でないかを疑う必要がある。 DHCP サーバの偽装はあまりに容易であり，正しいDNS 検索サーバのIP アドレスが設定されているか，常に確認するようにすべきである。特に無線LAN には警戒が必要である。

できることなら，DNS 検索サーバは自分で用意したものを使いたい。プロバイダのDNS 検索サーバも信用できない

2. ルートサーバは本物か

ルートサーバのIP アドレスのリスト（ルートヒントファイル）が信用できる入手経路を経た最新のものになっている必要がある。最近では 2007 年 11 月に L.root-servers.net のIP アドレスが変更になっている。

FTP を信用するならば，

ftp://ftp.rs.internic.net/domain/named.root

で入手できるが，あなたのDNS を信用する必要があるのがつらいところである。ちなみに筆者の環境では，このサーバのIP アドレスは 198.41.0.6 である。

ルートヒントファイルはウィルスに書き換えられる危険性も考慮しておく必要がある。

3. ルートサーバの管理は信用できるか

恐ろしいことにルートサーバに，いくつかの国のTLD のDNS サーバのIP アドレスが間違って登録されていたことがあり，それによりハイジャックの危険性があった。このようにルートサーバも信用できないことを承知しておく必要がある。

4. TLD は信用できるか

TLD のDNS サーバも信用してはならない。セキュリティ勧告に従わず， DDoS 攻撃の踏み台になったり，毒入れ（偽のデータを注入）される危険性のあるサーバを運用しているTLD がいくつもある。 TO もそのひとつであるが，DNS サーバのひとつがまるで信用できない動作をしている[*2]。

こうしたTLD の大部分は，文献 3 の図に示されるようにDNS サーバを相互に依存しあっており，自ドメインの運用を十分な責任を持って運用しているとは言い難い状況にある[*3] [*4]。

5. 個々のドメインは信用できるか

個々のドメインの信頼度に至っては，どうしようもなく悲惨な状況と言って良いだろう。

機能していない，毒入れ可能， DDoS の踏み台，はてはハイジャック可能まで問題のないドメインを探す方が困難なくらいである[*5] [*6]。

最悪なケースとしては visa.co.jp をはじめとするいくつかのドメインが筆者の管理下になってしまった事件がある[*7]。

6. DNS の通信は信用できるか

DNSは通信相手の認証を行っていない。このためDNS検索サーバはうまく偽装された応答を安易に受け取ってしまう。

これが毒入れであるが，毒入れの容易さはDNS検索サーバの実装にも依存する。毒入れの容易な実装については，セキュリティ勧告がいくつもでており，そうした脆弱なものを使わないことが肝要であるが，自分が用意したDNS検索サーバでない限りその確認は困難かもしれない。また，毒入れの容易さは，検索対象のドメインの設定にも依存するが，これは自ドメイン以外はただただ文句をいうしかないだろう。

7. インターネットはひとつか

そもそも世界のすべての人が同じルートサーバ配下の同じ名前空間を利用しているということ自体が幻想である。ICANN以外の名前空間や，別なルートサーバ(Alternate Root)を支持している人たちは存在するし[*8,*9]，中国のブラウザはICANNのルートサーバには存在しないTLDを受けつけるように見える（実際はトリックによりSLDをTLDに見せかけている）。NTT東西やNTTドコモなどが自社網内で独自に運用しているドメインを利用したことのある人もあるだろう。

また，米国商務省の管理下（のICANNの管理下）にあるルートサーバと名前空間を国連に移管すべきという国際的な政治摩擦が，2006年にはインターネット分断か？という事態にまでエスカレートしていたことは，日本国内ではあまり報じられていない。

以上のように，インターネットの基盤であるDNSにおいて真正性は幻想であり，電子証明書などの別の基盤に真正性を求めない限り，接続相手は常に偽者でありうることを前提にせざるを得ないことを肝に命じて欲しい。

幻想としてのルーティング

DNSを用いず，あるいは運良くDNSで通信相手の正しいIPアドレスが得られたとしよう。あなたはあなたの期待する本物の通信相手と通信できるだろうか。

インターネットにおいて，あなたの発した電文はIPパケットに分割されて，いくつものルータに中継されて相手に届く。このとき，個々のルータは自分が受けたIPパケットを，次にどのルータに受け渡したら良いかを，経路表に照らし合わせて判断する。これがルーティング＝経路制御である。経路表はインターネットにおける地図のような役割を果たすわけである。ルータはお互いに自らの知っている経路表を交換し，補完しあうことにより，世界への地図を得ている。

A-B-C-D-E

というネットワークがあるとしよう。

ルータCは，Bの先にAがあることをBから伝えられ，それをDに伝える。Cはまた，Dの先にEがあることをDから伝えられて，それをBに伝える。こうして，Cは，Bを通してAに，Dを通してEにIPパケットを送ることができるわけである。

しかし，ここで，Eが自分はAであるという嘘の情報を流したらどうなるだろうか。Cからみると，ネットワークは，

A-B-C-D-A

というように見えることになる。ここで，問題になるのは，Cは，Bの先のAと，Dの先のAのどちらが本物か，経路表だけではわからないということである。もしネットワーク的にD側のAが近くに見えれば，Cはそちらと通信してしまうことになる。これを経路ハイジャックと呼ぶ。隣接するルータを認証する仕組みは存在するが，経路表自体には何の認証の仕組みもないので，2つ以上先のルータからの経路ハイジャックを防ぐことは容易ではない。実際，spamやフィッシングの偽装手段として経路ハイジャックが悪用されていることが報告されている。

対策として，IRR(Internet Routing Registry)という国際的なデータベースに各組織がもつ経路を登録しておいて，ルータがそれを参照することにより，経路の正当性を確認しようという仕組みも存在している。しかし，現在のところIRRに登録されたデータが不完全なため有効に

は機能していない。

こうした状況に対し，総務省が 2006 年度から 4 ヶ年計画で経路ハイジャック対策の研究に乗り出していたり，Telecom-ISAC Japan などが経路奉行[*9]という監視体制を整備しつつある状況である。

ともあれ，学校や家庭などの端末からは，経路がハイジャックされているかどうかなど知るよしもない。また，このような大掛かりな経路ハイジャック以前に，無線 LAN や管理の甘い LAN において，偽の DHCP サーバで偽のゲートウェイルータに誘い込むことは，あまりに容易である。

このように，DNS とインターネット基盤の双璧をなすルーティングにおいても，電子証明書などの別な基盤に真正性を求めない限りは，ひたすら幻想を信じつづけるしかないのが現状なのである。

なお，ついでに述べておくと，ルーティングについては，さらに危惧すべき問題がある。2011 年には IPv4 アドレスの在庫が枯渇することが予測されており，アドレスを得られなくなったインターネット後進国が堂々と経路ハイジャックを行ってくる（先進国と同じ IP アドレスを使い出す）ことも危惧されている。

また，IP アドレスブロックが細かく分割されて取引されるようになり，経路表の容量が膨らんでルータがパンクする事態も危惧されている。こうなってくると，Integrity のみならず，Availability ＝可用性にも大きな支障が出てくることにもなる。

侵入を防止することは可能か

ここまではインターネットにおいて，通信相手の真正性について述べてきた。すでに，ここまででセキュリティについて，かなり悲観的な印象を持たれたことと思うが，セキュリティとは 100% の安全を求めることではない。むしろインシデントはどうしたって十分に起こりうるという前提に立つことがセキュリティ対策の第一歩であり，本論の目的は，その前提の確認に過ぎないことをお断りしておきたい。

さて，次に論ずるのはインターネットと接続した組織における外部からの侵入防止についてである。実は，この章ではあまり多くを述べることはない。あえて言えば読者の皆様の期待を裏切るための章かもしれない。

すでに述べたように，通信相手の真正性を IP パケットのレベルで確認することは，後述する電子証明書なくしては，原理的にみて不可能に近いといっても良い。相手の真正性の判断ができないのに，相手によって，侵入を許可したり拒否したりということが有効にはなり得ないのである。

ファイアーウォールで不要なサービスに対する通信は相手によらずすべて遮断してしまえば良いという考えはあるだろう。しかし，問題は利用したいサービス，例えば HTTP, HTTPS, DNS, SMTP, SSH, FTP 等々をどうするかなのである。悪意ある侵入はこうした一般的な通信でこそ行われる。これらを開け，他を塞ぐことにどれほどの意味があるのだろうか。
色々新しいものを生み出してもらいたい若い世代を，オールドファッションな通信だけの世界に閉じ込めることに意味はあるだろうか。

インターネット哲学はさておいても，検討すべきなのは，ネットワークへの侵入防止よりも，機器 1 台 1 台への侵入防止であり，また，侵入防止よりも，自組織が踏み台となって外部に迷惑をかけることの防止に力を入れるべきである。

他の指南書にあるような，多様なアクセスコントロールについては本論では述べない。くどいようであるが，インターネットにおいて通信相手の真正性を DNS や IP パケットレベルで確認することは不可能に近いからである。最近問題となっている攻撃として，JavaScript や Flash など，ブラウザ上の通信機能を踏み台にして内部へ侵入，攻撃を仕掛ける DNS Rebinding Attack[*10] という手法が知られている。これに対してはいまのところ内部同士の通信も信用しないという対策しかない。

機器への侵入防止はひとえに，不要な通信サービスは止めること，脆弱性の判明しているソ

フトウェアを使わないこと，そして後述する認証を内部外部問わずしっかり行うことである。

脆弱性情報に関してはJPCERT/CC[*11]のWebサイトやそのメーリングリスト，また各それぞれのソフトウェアのベンダからの情報を密に確認することをお薦めする。

次に外部に被害を及ぼす踏み台の防止について述べる。多様な踏み台被害が考えられるが，ここでは現在もっとも深刻な問題となっているspamとDNS amplificationによるDDoSに言及する。

spamの最大の被害は迷惑な内容のメールを読んでしまうことではない。宛先不明となったエラーメール（バウンスという）が，詐称された差出人のもとへ世界中から殺到し，メールサーバや回線がパンクしてしまうという被害が問題なのである。この問題が十分に認識されていないために，俺はspamは気にならないのだから，余計な対策をするな，という話がまかり通ってしまう。

spamはインターネットの可用性に対する最大級の脅威であり，徹底した態度で対策に望まなければならないのである。特に詐称された宛先へのバウンス（バックスキャッタという）対策が必要である。メールを受信してからspam判定する方式では，バックスキャッタが発生する可能性があるため，SMTPセッション中にspam判定を行う方式を採用する必要がある。

次にDNS ampについて述べる。DNS ampとはDNS amplification attackの略称であって，文字通りDNSの通信を増幅することによる攻撃である。

DNS ampで踏み台になるのは，アクセス制限されていないDNS検索サーバである。DNS検索サーバはDNSキャッシュサーバとも呼ばれるが，これは一度検索したデータをキャッシュするからである。攻撃者は数多くのDNSキャッシュサーバたちに，容量の大きなデータを検索してキャッシュさせておき，被害者のIPアドレスを装って，これらのサーバ群に一斉に検索をかける。すると問い合わせパケットの数十倍から最大200倍近くのサイズの応答パケットが，被害者を襲うことになる。

DNSキャッシュサーバを運用している管理者は，自組織内部からの問い合わせのみに応答するようアクセス制限をかける必要がある。

しかしながら筆者の調査[*5]では対策されていないサーバが8割を越える悲観的状況にある。

安全を守るための暗号技術

暗号はConfidenciality＝機密性のためにあると考えられているようであるが，ここまで述べてきたように，まず大切なのはIntegrity＝真正性である。いくら通信路の暗号化をしてみても通信相手が偽者であれば，意味はない。相手の真正性を確認するためにこそ暗号は必要であり，暗号を用いて通信相手の認証を行わない限り，インターネットのセキュリティは保全のしようがないのである。

暗号をWWWに応用したHTTPSを例にとってみよう。このHTTPSの利用に際して，いくつか世間には誤解があるようなので，その誤解をここで解いておきたい。

一つ目の誤解は，クレジットカード番号など重要なデータを送信する際に最も重要なのは暗号化であるという認識である。

多くの場合，情報漏洩は回線上での暗号解読，いわゆる盗聴によってではなく，成りすましによって偽のサーバにデータを送信させられてしまうことによって生ずる。従って，最も重要なのは暗号化よりも相手の認証なのである。そして，その認証を確実にするためには適切な電子証明書が適切に設定されていることが重要である。

しかし，世間では電子証明書は暗号鍵のおまけのように考えられており，期限切れの証明書や，信用できる署名のない電子証明書によって運用されているサイトをよく見かける。不適切な電子証明書であっても暗号化しないよりはましだろうという誤った認識のせいであろう。ブ

ラウザが警告を出すような電子証明書を使っていながら，暗号化のためだから警告を無視せよと指示しているサイトすら存在する。しかも，それが銀行だったり，自治体だったりするのが情けない。ブラウザが警告を発したときは，決してその先に進んではいけない。

２つめの誤解は，重要なデータをフォームから送信する際にだけHTTPSが必要であるというものである。成りすましによって，偽の情報を流されたくないサイトは，「本来は」すべからく信用できる電子証明書を備えるべきなのである。だが，問題はこの「本来は」にある。あなたのサイトの閲覧者が，あなたの正しいサイトはHTTPSで運用されているということを知っていなくては意味がないのでである。

さらにやっかいなのはインターネットに接続する多くの人々の意識である。ここまで電子証明書の重要性を書いてきておいて，前言をひっくり返すようなことを続けて書くのは心苦しいのであるが，電子証明書を容易に信用してはいけない。

ブラウザが警告を発しない場合，そのサイトはそのブラウザのベンダーがお墨付きを与えた認証局（あるいはその配下の認証局）によって署名された正当な電子証明書を持っているということであり，技術的な観点からは信用していいというだけのことである。

問題はブラウザが判定してくれるのは電子証明書がそのドメインのものであるということにすぎないということである。ブラウザはそのサイトが「あなたの思っているサイトである」ということは判定してくれない。

あなたはあなたの利用している銀行の正しいドメイン名をご存知だろうか。

まとめ

つまるところ，安全・安心なインターネットなどというものは幻想である。一部のサイトが立派な運用をしてみたところで，大多数のサイト（ルートサーバでさえも！）が信用できない運用をしている現状において，インターネットに接続する一般の人々に「疑わしいサイトには近づくな」というアドバイスは無益なのである。大多数のサイトが正しく信用できる運用をして，初めて一部の疑わしいサイトの判別ができるようになるのである。

インターネットは魑魅魍魎が跋扈する無法地帯であることを認識，啓蒙していかなくてはならない。こうすれば安心などという欺瞞はいけない。安心しないことこそが，安全への近道であり，インターネットに接続する人たちは，常に自分の頭で考え，リスクを判断し行動すべきである。

以下はあくまで私の個人的な持論であるが，インターネットは自由な空間でなくてはならない。安全，安心を，法や権力に求めることは自由の放棄である。必要なのは自由の下の自律と協調である[*12] [*13]。その確立が不可能であるならば，インターネットが幻想のまま崩壊するのもやむを得ないだろう。監獄になるよりはましである。

参考文献

[1] http://www.icann.org/
[2] http://d.hatena.ne.jp/memecomputing/20070930
[3] http://www.e-ontap.com/dns/map/
[4] http://www.cs.cornell.edu/people/egs/beehive/dnssurvey.html
[5]「DNSの危機的状況」,鈴木常彦，2007,「FIT2007（第6回情報科学技術フォーラム）一般講演論文集，第4分冊，pp. 29-31,.
[6] Rikitake, K., Suzuki, T. and Nakao, K, DNS Security: Now and The Future, IEICE Technical Report ICSS2007-01, pp.3-8 (2007)
[7] http://www.e-ontap.com/summary/
[8] http://www.new.net/
[9]http://european.ch.orsn.net/
[10] http://crypto.stanford.edu/dns
[11] http://www.janog.gr.jp/meeting/janog19/files/irr.pdf
[12] イヴァン・イリイチ,「コンヴィヴィアリティのための道具」,日本エディタースクール出版部,1989
[13]佐伯啓思,「自由とは何か」,講談社,2004