

インターネットの新たな問題

長谷川 明 生

．ネームサービスの問題

ある日、海外からSPAMメール（大量のゴミメールをばら撒く行為のこと）に関する情報が電子メールで届きました。最初SPAMの苦情だとばかり思い込んでいましたので、削除しようとしてきました（差出人アドレスのデタラメなメールが多発していますので）が、「消す前に、目をとおしてください。苦情メールじゃありません」という声がありました。

中身を読むと、「SPAMに関係するドメインのネームサーバとして、NICEのIPアドレスのホストが登録されている」という指摘です。実際に、nslookupすると、ホスト名は別として、2台登録されているネームサーバの1台のIPアドレスが133.6.mmm.nnnとなっています。念のために「COM」ドメインのルートネームサーバ（DNSツリーの大元の1台）で検索しても、たしかに133.6.mmm.nnnが返ってきます。そこで、インターネットのwhoisで、ドメイン名登録業者の管理している登録情報を検索してみました。すると、やはり133.6.mmm.nnnがネームサーバとしてデータベースに登録されています。

これだけなら、学内のだれかが勝手にネームサーバを起動して、登録した可能性も考えられます。しかしながら、133.6.mmm.nnnというアドレスは、現在NICEで未使用のアドレスブロックのもので、仮に、このようなアドレスのホストがあっても、どこからも到達できません。

間違いという可能性もありますが、問題の情報が故意に登録されたとすると、DNSシステムの情報そのものに問題が潜んでいることになります。もっとも、ドメイン名の取得や利用もお金を払うだけで、誰でも可能となっているわけで、インターネットの旧来の善意に基づいた管理が保たれていると考えるのがノーテンキすぎるのかもしれませんが。

そんな話を知人に愚痴ったら、知人は、「僕は、まったく知らないxxドメインの公式管理者として、インターネットのwhoisデータベースに登録されていましたよ！」とっていました。赤の他人から、「xxドメインのネットワークの設計をどうしよう？」という彼にとっては意味不明かつ寝耳に水な英文のメールが届いて、びっくりしてwhoisを検索してみたら、そのとんでもない登録にぶつかったということでした。ひょっとしたら、私の名前も、まったく私が関知しないところで使われているのかもしれませんが。でも、知人が経験したような、ちょっとした出来事がないかぎり、名前を使われていたとしても、それを知ることすらできません。知人のその「トンデモない」登録が修正されたかどうかまでは聞きもしました。

これらのことから、インターネットの権威があると思いついて（筆者だけが、勝手に思いついていたのかもしれませんが）データベースの中身が、結構問題がありそうだということに気

づかされました。

・セキュリティ証明書は

そこまで考えたところで、インターネットのWebの暗号化に使われる証明書は大丈夫かと不安になりました。日常的に、ソフトウェアの利用者登録やアンケートの現場で、SSL (Secure Socket Layer) の暗号用鍵と証明書がセットで使われています。暗号化通信開始時には、セキュリティ証明書を受け入れるかどうか選択肢が提示されます。私も含めたたいの人は、何も考えずに「はい」を選択していることでしょう。つい面倒なので「xxx社からの証明書を以後信頼する。」といったチェックボックスにチェックしてしまうこともあります。

でも、よく考えてみると、「証明書」は、そのWebサーバが「証明書」を証明業者から取得して持っているということだけを主張しているにすぎず、Webのコンテンツを保障しているものではないという事実に行きあたります。私たちは、「証明書」や「身分証明書」というモノを見せられると、つい安心しがちですが、Webページの内容を一片の「証明書」だけで無批判に受け入れることがないように注意する必要があります。

・公開鍵の管理

メールの機密を保つためにPGPといったものが使われています。PGPでは、秘密鍵と公開鍵をペアで使います。で、公開鍵の方を、相手に送って、これでメッセージを暗号化してもらいます。よほど特殊な人でもないかぎり、相手ごとに暗号を変えるといった面倒なことはしないでしょ。というわけで、誰かを相手に暗号化をしたとたんに、鍵は、どうしても友達の輪を通して拡散してしまいます。

このような環境では、秘密鍵の管理は厳重にしなければ意味がありません。さらに、安全を考えると、パスワードの更新が必要なと同様に、鍵ペアも定期的に更新すべきです。さて、そこで、ネットに流れた古い鍵の回収をどうするかという難問にぶつかります。みんなが、新しい鍵に変えてくれないかぎり、いつまでも古い鍵が残ることになります。また、古い鍵の保存期間をどうするかといったことに悩みます。

・結論

インターネットは一般社会と同じです。直接顔が見えず、数も多いだけに、街の雑踏より大変かもしれません。そんな場所で迷子になったり、迷子を出してしまったらどうしようもありません。インターネットに流れた情報は、迷子やボヘミアンです。そのような中で、どう振舞うかは、利用者が自己責任で決めなければならないことです。

どうであれ、インターネットは、すべて自己責任の世界であることを再確認させられた、ここ数ヶ月でした。

(はせがわ あきうみ：名古屋大学情報連携基盤センター大規模計算支援環境研究部門)