第19部

DNS extension and operation environment（DNS）

関谷 勇司、石原 知洋

第１章　はじめに

DNS WGでは、DNSにおける実装上や運用上の問題点に関して、情報共有とそれを解決するための活動を行っている。2022年度はメールセキュリティにおけるDNSについて重点的に調査や議論を行い、また東京大学において開催されたメールセキュリティについてのシンポジウムにおいて発表を行った。

第２章　メールセキュリティとDNS

現在、メールを取り巻くセキュリティ状況は悪化の一途をたどっている。また、誤送信やマルウェア感染による、意図しないメール送信による情報漏えい事故も頻発している。さらに、迷惑メールの増加にともない重要なメールを見逃すという悪循環が発生している。

電子メールのセキュリティは以前からPGPやS/MIMEなどのend-to-endによる保護が提案されて使われているが、広く普及しているとは言い難い状態である。また、end-to-endの保護はお互いに認識している相手についてその機密性や完全性を確保できるが、電子メールはあらゆる相手から送信されうるという特性から、End-to-Endのメールセキュリティのみでなりすましや詐称、スパムなどを防ぐことは困難である。

メールシステムに対しての攻撃は発信側に対して攻撃を行いメールを盗み見たり改ざんしたりする攻撃と、受信側に対してなりすましメールやスパムなどを送信する攻撃に分けられる。発信側に対する攻撃への対策としては、MTA-STSやDANEなどのMTA間の通信を信頼できるものにする対策が提案されており、また、受信側に対する攻撃の対策としてはSPF、DKIM、DMARCなどの送信者の認証やメールコンテンツを署名する仕組みが提案されている。

これらの方策はDNSのTXTレコードを用いており、強くDNSに依存している。また、メール配送に利用されるMXレコードの安全性も当然ながらメールの安全性に直結する問題となる。しかしながら、DNSレコードの保護を行うDNSSECは特に日本において広く普及しているとは言いがたく、メールシステムを様々な手段で保護してもDNS自身が脆弱な攻撃対象として狙われうることとなる。

シンポジウムではこれらの問題について発表、注意喚起を行った。また本発表ののちにメールセキュリティについてのパネルディスカッションが行われ、DNSについては下記のような意見や質問が寄せられた。現状ではなかなかDNSSEC導入に踏み切ることが難しいという意見が多く、今後の普及については継続的に議論を行っていく必要がある。

第３章　質疑一覧

: DNSSEC validationを入れた場合に何らかの副作用がある可能性があり、コストとリスクに対して現在のところ利点が乏しいように思える

: ac.jpでDNSSECを実装する場合にDSをどうやって登録すればいいのかなどの情報が少ない。自動化できるのか、情報がないので、絵に描いた餅みたいになっていると思う。例えば東大でDNSSECをしているならばその方法を教

えて欲しい。BINDを動かしていてそこで設定する、などというやり方だと現実的に事務作業員が業務で定常運用に載せるのは難易度が高いのではないか。

: 大学の先生などは多段のメール転送ができてあたりまえと思っている人も多く、なかなか転送禁止を強制するのは難しいなと感じる。また、転送と旧来のメーリングリスト（Subjectに通し番号を入れ、Fromはそのまま）が組み合わさるとDKIMもSPFも失敗してしまうのでDMARCのポリシーを絞ると自分のメールが届かなくなるのも問題である。自組織の対策を進めると自組織に害があるため移行が進まないという面もあるような気もする。

: メールセキュリティ技術やDNSSECの導入についてはどこかの国の機関が旗を振ってガイドラインなどを作る必要があるのでは