SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

逆引き DNS の登録状況と DNSSEC の暗号アルゴリズムに関する実態調査
Field study of registration status of Reverse DNS and cryptographic algorithm of DNSSEC

山口　詩織 *　　岡田　雅之 †
Yamaguchi Shiori　　Okada Masayuki

キーワード　DNSSEC　DNS　逆引き DNS　IP　暗号アルゴリズム　楕円曲線暗号

あらまし

インターネットを活用する上で、DNS の名前解決は必要不可欠なテクノロジーである。しかし、インターネットの基盤技術としてすでに 30 年以上に渡って使われ続けている DNS は、コンピュータやネットワークの能力や信頼性がまだ低かった時代に設計されたため、処理にかかる負担を極力軽くすることを目的とした UDP 通信などのシンプルな設計となっている。[1] このことに起因する弱点を突いた攻撃は毎年のように発生している。DNS の偽造応答によるキャッシュポイズニング攻撃は、攻撃対象者に対して悪用サイトへの誘導やメールの盗聴や Web サイトの改竄、スパムメールの送信などが可能となる。

2008 年 7 月に、AT&T の ISP が運営する DNS キャッシュサーバが攻撃対象となった事件がある。[2] この攻撃により、その DNS キャッシュサーバの利用者が Google サイトにアクセスすると 404 エラーが表示される問題が発生した。根本的な解決策として、やりとりするデータの信頼性を高めることにより、キャッシュポイズニング攻撃を防ぐことができる DNSSEC(DNS Security Extension) が開発された。しかしながら、DNSSEC 利用率は途上であるという事実がある。

ドメイン名から IP アドレスを検索することを特に正引き DNS と呼び、正引き DNS に対して IP アドレスから DNS の検索を行うことを逆引き DNS と呼ぶ。ドメイン名から IP アドレスを検索する正引きについては、そのわかりやすい重要性から、DNSSEC の導入状況などについて複数の研究、調査が行われている。

一方、逆引きにも DNSSEC がある。逆引き DNS とは、IP アドレスの情報から該当の IP アドレスに関する何らかのドメイン名に関する情報が登録され、電子メールの接続の際や ssh でのログインの際、主に接続元がどのようなネットワークかを判断するために活用されているといわれている。具体的には、電子メールを転送する際に利用される SMTP の接続の際、接続してきたコネクションの接続元の IP アドレスについて、逆引き DNS 問い合わせを行い、得ることのできた応答を活用して電子メールの受信、中継の可否を判断する。また、ssh などのログインの際には、同じく接続元に関係するドメイン名を取得できるかどうか、または、特定の文字列を含むか、などを根拠にログインの許可、不許可を判断する。IP アドレスから何らかの文字列を検索する逆引き DNS については、その利用実態や登録の状況については継続した調査が行われておらず状況が不明となっている。

本研究は、Regional InternetRegistry(RIR) の公開ファイルから得られたネットワーク単位での IP アドレスにおいて逆引き DNS から様々なリソースレコードを逐一問い合わせる方法によって、逆引き DNS の登録状況及び DNSSEC の利用状況を 44ヵ国に選択し、国別で調査した。加えて、DNSSEC に使用している暗号アルゴリズム番号の識別から公開鍵暗号である RSA と楕円曲線暗号 ECDSAP、及び RFC8624 で推奨されていない暗号アルゴリズムの使用割合を得た。また、DNSSEC の DNSKEY レコードの応答エラーから DNSSEC を誤って導入をしている傾向を発見し、これらの調査の報告を行う。

* 長崎県立大学情報セキュリティ学科 4 年, University of Nagasaki, bs218040@sun.ac.jp
† 長崎県立大学情報セキュリティ学科教授,University of Nagasaki, okadams@sun.ac.jp

[1] あきみち、空閑洋平、『インターネットのカタチ もろさが織り成す粘り強い世界』、株式会社オーム社 (2014 年 5 月 20 日第 1 版第 4 刷発行) 引用

[2] 『DNS の脆弱性問題で ISP に被害』 https://www.itmedia.co.jp/enterprise/articles/0807/31/news021.html