DNSセキュリティ機構の普及状況調査：現状と今後の課題

矢島 雅紀[1,a)]　千葉 大紀[2]　米谷 嘉朗[3]　森 達哉[1,4]

概要：DNS アンプ攻撃，DNS キャッシュポイズニング攻撃のように，DNS をターゲットとした攻撃の脅威は衰えることをしらない．また，フィッシングサイトやマルウェア配布サイトなど，偽ドメイン名の判定の困難性を悪用した攻撃は依然として猛威を奮っている．これらの DNS に関連した脅威に対する有効な対策として，様々な DNS セキュリティ機構が提案され，標準化と実装が進んでいる．しかしながら，これらのセキュリティ機構がインターネットの DNS エコシステムにおいてどの程度普及し，どの程度有効に機能しているかは明らかではない．このような背景をもとに，本研究は主要な DNS セキュリティ機構である DNSSEC，DNS Cookie， CAA， SPF， DMARC， MTA-STS， DANE， TLSRPT を対象とし，それらの普及状況に関する大規模な調査を行う．さらに，DNS オペレータに対するオンライン調査を実施し，その理由を明らかにすることを狙いとする．この結果，全体として多くの DNS セキュリティ機構の普及率は低い状況にあること，そしてより設定難易度が高いセキュリティ機構ほど普及率が低いことが定量的に明らかになった．セキュリティ機構の設定状況が，設定難易度に影響を受けることはオペレータに対する調査結果によっても支持された．これらの知見は DNS セキュリティ機構を普及させる上で，導入が簡単な仕組みが重要であることを示唆している．

キーワード：DNS Security，Measurement

Measurement Study of the Adoption of DNS Security Mechanisms †

Masanori Yajima[1,a)]　Daiki Chiba[2]　Yoshiro Yoneya[3]　Tatsuta Mori[1,4]

Abstract: The threats targeting DNS, e.g., DNS cache poisoning attacks and DNS amplification attacks have continued to be vital in the wild. In addition, attacks using the domain name fraudulent such as phishing websites have continued to be a significant threat. In response to these backgrounds, various DNS security mechanisms have been proposed, standardized, and implemented as effective countermeasures against DNS-related attacks. However, it is not clear how widespread these security mechanisms are in the DNS ecosystem and how effectively they work in the wild. With this background in mind, this study targets the major DNS security mechanisms deployed for the DNS name servers, DNSSEC, DNS Cookies, CAA, SPF, DMARC, MTA-STS, DANE, and TLSRPT, and a large-scale measurement analysis of their deployment is conducted. Our measurement study quantitatively reveal that, as of 2021, the adoption rate of most DNS security mechanisms, except SPF, remains low, and the adoption rate is lower for mechanisms that are more difficult to configure. These findings suggest the importance of developing easy-to-deploy tools to promote the adoption of security mechanisms.

† The full version of this work will be presented at IEEE GLOBECOM 2021.

Keywords: DNS Security, Measurement

1. はじめに

DNS [6] はインターネットの重要なインフラストラクチャの 1 つである．DNS は，インターネットアクセスの

[1] 早稲田大学 / Waseda University
[2] 日本電信電話株式会社/ NTT
[3] 日本レジストリサービス/ JPRS
[4] 情報通信研究機構 / NICT
[a)] y-masa22@nsl.cs.waseda.ac.jp

基盤的役割を果たしており，様々な攻撃を受ける脅威に晒されている．DNS を標的としたセキュリティ脅威は，以下の 3 つに分類することができる．1 番目の脅威は，DNS サーバを対象とした脅威である．例えば，DNS の応答を書き換えることを目的とした DNS キャッシュポイズニング攻撃 [19]，および DNS サーバのオープン性を悪用した DNS アンプ攻撃を始めとする DDoS 攻撃 [1] などが挙げられる．2 番目の脅威は，DNS が扱う名前を対象とした脅威であり，偽のドメイン名を用いたフィッシングサイトやマルウェア配布サイトなどが挙げられる．3 番目の脅威は，DNS クエリ情報に含まれるプライバシー情報の漏洩である．例えば，オープンアクセスの無線 LAN において，ユーザのクエリが中間者によって，盗聴，改ざんされるリスクがある．

これらの脅威を緩和することを目的として，様々な DNS セキュリティ機構が提案，標準化，実装されてきた．例えば，1 番目の脅威に対する対策として，DNSSEC，DNS Cookie が，2 番目の脅威に対する対策として，CAA，SPF，DMARC，MTA-STS，DANE，TLSRPT[*1]が，3 番目の脅威に対する対策として，DNS over TLS (DoT), DNS over HTTPS (DoH) がある．これらの対策は DNS サーバの更新が必要なもの，DNS レコードを追加することで対応できるもの，エンドユーザが利用するクライアントで動作するものまで様々である．

本研究は，以下の研究的問い (RQ) にこたえることを狙いとする．

RQ: インターネット全体における DNS セキュリティ機構の普及状況はどのようなものか？普及を妨げる要因があるとすればそれは何か？

本研究は権威 DNS サーバで動作するセキュリティ機構に着目する．スタブリゾルバとフルリゾルバの間で機能する DoT や DoH，QNAME minimization の調査は本研究のスコープ外である．本研究の新規性は，複数の DNS セキュリティ機構を横断的に調査する点にある[*2]．これまで，DNS Cookie [11]，DNSSEC [10]，DANE [17] といった，個別の DNS セキュリティ機構を調査した研究事例は存在するが，セキュリティ機構全体を対象とした調査事例は過去に存在しない．このような調査により，それぞれのセキュリティ機構が普及しやすい，あるいは普及しにくい理由を探ることが可能となる．

上述した RQ に答えるために，セキュリティ機構の普及状況を大規模に調査する．本研究では，DNS の最も重要な部分ともいえるルートドメイン，分野ごとに割り当てられる 22 個の gTLD，国ごとに割り当てられる 254 個の ccTLD，普段多くの人に利用される有名なドメイン名 9,999 個に対して調査を行った．これらのドメイン名に対する IP アドレスは全部で 13,434 個である．具体的には，人気が高いドメイン名の名前解決を担う権威 DNS サーバを対象とし，各セキュリティ機構の普及率，各セキュリティ機構の普及率の相関，およびセキュリティ機構の設定難易度と普及率の相関を調査する．さらに，DNS セキュリティ機構が普及しない理由を明らかにすることを目的として，DNS サーバを運用しているオペレータを対象に予備的オンラインサーベイを実施した．

本研究の貢献，および得られた主要な知見は以下のとおりである．

- DNS セキュリティ機構の普及状況を実インターネットで網羅的に調査した初の研究である．
- 人気が高いドメイン名において，SPF 以外のセキュリティ機構への対応率が低い傾向にあることを明らかにした．
- 広く知られているセキュリティ機能については，設定が容易なものほど普及率が高い傾向にあることを明らかにした．

2. 背景

2.1 DNS サーバへの攻撃を緩和するセキュリティ機構

DNS サーバに対する攻撃を緩和するセキュリティ機構として，DNSSEC と DNS Cookie がある．以下にそれぞれの概要を示す．

DNSSEC DNSSEC [23], [24], [25] は，DNS 応答の完全性を保証するメカニズムである．DNS 問い合わせの応答に電子署名を付けることで，応答が改竄されていないか検証を行うことができる．電子署名の検証に用いる公開鍵は，親ゾーンで公開され，親子のゾーン間の信頼の連鎖を構築する．DNSSEC はあくまで応答の完全性のみ保証する．したがって，通信の相手が秘密裏にすり替わっている場合に対応することができない．そのようなケースは，以下で示す DNS Cookie で対応することができる．

DNS Cookie DNS Cookie [7] は，DNS クライアントとサーバの双方が，通信を行う相手がすり替わっていないことを検証可能にするメカニズムである．クライアントとサーバはそれぞれが DNS Cookie を検証する．検証に失敗した場合，サーバは BADCOOKIE エラーで応答し，レートリミットを適用するか，パケットを破棄する [7]．この機能により，名前解決のパケットを観測することができないオフパスの攻撃者は，正しい DNS Cookie を持つ偽のクエリや応答を生成することが極めて困難となる．すなわち，DNS Cookie を導入することにより，DNS キャッシュポイズニング攻撃や，DNS アンプ攻撃を抑制できる．

[*1] これらの機能については 2 節で述べる．

[*2] 著者らが 2021 年 3 月に ICSS 研究会で発表した研究 [28] との差分は以下の通り．(1) 調査対象を権威 DNS サーバにフォーカスし，メールに関するセキュリティ機構の普及率を追加調査 (2) 設定難易度と普及率の相関関係を分析 (3) 普及が進まない要因に関して，DNS オペレータに対するユーザスタディを実施

表 1　DNS セキュリティ機構を利用する際に設定する DNS レコード

	設定箇所	設定するドメイン名	RR	シグネチャ
CAA	server	<domain name>	CAA	n/a
SPF	sender	<domain name>	TXT	v=spf1...
DMARC	sender	_dmarc.<domain name>	TXT	v=DMARC1...
MTA-STS	receiver	_mta-sts.<domain name>	TXT	v=STSv1...
DANE	receiver	_25._tcp.<mail server domain name>	TLSA	n/a
TLSRPT	receiver	_smtp._tls.<domain name>	TXT	v=TLSRPTv1...

2.2　偽ドメイン名の脅威を緩和するセキュリティ機構

現在のインターネットにおいて，ドメイン名の主要な用途は，ウェブと電子メールである．いずれのサービスも，フィッシングサイトやマルウェア配布サイトなどがもたらす脅威に晒されている．このような脅威を軽減することを目的としたセキュリティ機構として，TLS 証明書の発行にかかる制限をつけた CAA，および電子メールを送受信する際のセキュリティ機能を拡張する SPF，DMARC，MTA-STS，DANE，TLSRPT がある．表 1 に，それぞれの機能を利用する際に設定する DNS レコードをまとめた．以下に，それぞれの機構の説明を示す．

CAA DNS CAA レコード [12] は，第三者が TLS サーバ証明書を勝手に発行することを防止するためのメカニズムである．ドメイン名の管理者は，CAA レコードを設定することにより，登録ドメイン名の TLS 証明書の発行を許可する認証局を指定することができる．

SPF Sender Policy Framework (SPF) [26] は，メールの送信元の正当性を検証する仕組みである．管理者は DNS の TXT レコードに SPF の情報を登録することにより，当該ドメイン名に対して電子メールの送信を許可する IP アドレスを明示的に指定することができる．

DMARC Domain-based Message Authentication, Reporting, and Conformance (DMARC) [16] は，SPF および，DKIM [15] の 2 つの機能をもとに，送信元の正当性を判定する仕組みである[*3]．DMARC は，SPF と同じく，メール送信元ドメイン名の権威 DNS サーバにて TXT レコードを設定することによって利用することができる．

MTA-STS 一般に SMTP は通信を暗号化しない．STARTTLS [13] を利用することにより，メールの送受信を暗号化することができる．Mail Transfer Agent Strict Transport Security (MTA-STS) は，STARTTLS を電子メールの送信元に強制する仕組みである．

DANE DNS-based authentication of named entities DANE [9] は，メールの送信先の正当性を保証し，また，メールの機密性を保証する仕組みである．正当性の判定は DNSSEC を用い，また機密性は STRTTLS を用いる．DANE を利用するには，電子メールサーバに TLS の公開鍵を DNS の TLSA レコードとして設定する必要がある．

TLSRPT MTA-STS や DANE にて認証に失敗した結果，メールが届かない可能性がある．その場合に，失敗したことを伝えるレポートを受け取る機能が TLS Reporting (TLSRPT) [20] である．

[*3] DKIM [15] は，電子メールに電子署名を付加することで電子メールの認証を行う仕組みである．一般に，ドメイン名が適切な DKIM レコードを持っているかどうかを，DNS サーバの設定を元に調査するのは難しい．なぜなら，ドメイン名の管理者が任意に設定できるセレクタを推測する必要があるからである．そのため，DKIM を調査対象から除外した．

表 2　収集したドメイン名と IP アドレスの数

	ドメイン名	IP アドレス
Root	1	13
gTLD	22	110
ccTLD	254	993
Popular	9,999	12,318

3.　調査手法

本節では，調査対象としたドメイン名の概要，およびセキュリティ機構の設定状況を判定する具体的な方法を示す．

3.1　調査対象ドメイン名

調査対象として，3 種類のドメイン名，(1) ルートドメイン (**Root**)，(2) トップレベルドメイン (**TLDs**)，(3) アクセス数が多い人気ウェブサイトに用いられているドメイン名 (**Popular**) を採用する．はじめに，対象のドメイン名の NS レコードを調べ，応答に含まれている IP アドレスを記録する．なお，本研究では，IPv4 のみに着目する．次に，収集した IP アドレスに対し，当該 IP アドレスを管理しているドメイン名の NS レコードを要求するクエリを送信する．その結果，不正な NS レコードを返した IP アドレスを除外する．また，一つのドメイン名が複数の NS レコードを持ち，複数の IP アドレスが存在する場合は，その全てが調査対象となる．

次に，それぞれの種類のドメイン名のデータについて詳しく述べる．また，調査対象となったドメイン名および IP アドレスの数を，表 2 にまとめる．

Root 本研究では，ルートドメイン “.” に対する権威 DNS サーバを調査対象とする．DNS サーバは `A.ROOT-SERVERS.NET` から `M.ROOT-SERVERS.NET` までで，対応する IP アドレスの数は 13 である．

TLDs TLD としては，legacy gTLD と ccTLD を対象とした．legacy gTLD は次に示す TLD である: `aero`, `asia`, `biz`, `cat`, `com`, `coop`, `edu`, `gov`, `info`, `int`, `jobs`, `mil`, `mobi`, `museum`, `name`, `net`, `org`, `post`, `pro`, `tel`, `travel`, `xxx`．調査対象となった IP アドレスは 110 個である．ccTLD は，`ac` から `zw` まで，254 個のドメイン名，993 個の IP アドレスを調査対象とした [14].

Popular 本研究では，有名な人気ドメイン名のリストとして，Tranco [4] が公開している上位 1 万個のドメイン名を採用した．このドメイン名リストを 2021 年 4 月 29 日に収集した．なお，リストに含まれていたルートサーバ `root-servers.net` のドメイン名を除外した．結果として，9,999 個のドメイン名を得た．これらのドメイン名に対応する IP アドレスは 12,318 個であった．

3.2 セキュリティ機構設定の判定

以下では，ドメイン名がセキュリティ機構を設定しているかを判定する方法を説明する．それぞれのドメイン名に対応する IP アドレス群に対して調査を実施し，少なくとも 1 つの IP アドレスがセキュリティ機構を設定していると判断できた場合，そのドメイン名がセキュリティ機構を設定していると判定する．

DNSSEC まず，各々の IP アドレスに対し，DNSSEC を利用することを表す DO (DNS OK) ビットを立てた DNS クエリを送信する．応答に RRSIG レコードが含まれていた場合，DNSSEC を設定済みと判定する．

DNS Cookie 各々の IP アドレスに対し，ランダムなクライアント Cookie を設定した DNS クエリを送信する．応答に有効な DNS Cookie が含まれていれば，DNS Cookie を設定済みと判断する．

CAA 各々の IP アドレスに対し，対応するドメイン名の CAA レコードを要求する．応答に CAA レコードが含まれていた場合，CAA を設定済みと判定する．

SPF, DMARC, MTA-STS, TLRRPT, DANE 各々のドメイン名に対し，SPF, DMARC, MTA-STS, TLRRPT, TLSA のいずれかのレコードを 参照するクエリを送信する．応答が表 1 に記載されているシグネチャにマッチすれば，各々のセキュリティ機構を設定済みと判定する．DANE については，MX レコードに記載されているドメイン名が調査対象となる．したがって，MX レコードに記載されているドメイン名のうち 1 つが TLSA レコードを設定していれば，DANE を設定済みと判定する．

4. 調査結果

本節では，はじめに，収集した DNS サーバに対して，各セキュリティ機構の普及率を調査した結果を示す．次にそれぞれのセキュリティ機構の普及率の相関，ならびに設定難易度と普及率の相関を分析した結果を示す．最後に，DNS を運用するオペレータに対してオンラインサーベイを実施し，セキュリティ機構の設定有無およびその理由を調査した結果を示す．

4.1 DNS セキュリティ機構への対応率

表 3 に，3.2 節に示したセキュリティ機構の普及率を示す．Popular については，上位 10, 100, 1,000, 5,000, 10,000 個のドメイン名に絞った場合の結果を示す．なお，電子メールに関連した 5 つのセキュリティ機構 (SPF，DMARC, MTA-STS，DANE，TLSRPT) は，いずれも当該ドメイン名が電子メールを受信するように設定されていることが前提となるため，MX レコードが存在したドメイン名および IP アドレスに対する割合を示した．全体として，DNS サーバ対する脅威への対策となる DNSSEC や DNS Cookie のようなセキュリティ機構は，ルートドメインや TLD の権威サーバなど，DNS の基幹にかかわるサーバでの普及率が高い一方，ウェブで利用されるドメイン名では高くとも 2 割程度の低水準に留まっている．また，予想された通り，ルートドメインや TLD 権威サーバはウェブや電子メールのサービスを提供することがほとんどないため，対応するセキュリティ機構の普及率も低い．一方，人気ドメイン名の方は，普及率が高いセキュリティ機構とそうではないセキュリティ機構が混在した．以下では，それぞれのセキュリティ機構ごとに特筆すべき傾向を示す．

DNSSEC 前述したように，ルートドメインや TLD の権威サーバといった，主要な DNS サーバにおける DNSSEC の普及率は比較的高い．一方で，一般のドメイン名についてはかなり状況が異なっている．特に，Popular 上位 10 個のドメイン名における DNSSEC の普及率が 0 であった．上位 1 万個のドメイン名全体においても，DNSSEC を設定して DNS サーバを運用していたドメイン名は，わずか 7.67%であった．これらの観測結果は，DNSSEC の設定難易度が高いという事実 [10], [18], [21] とも矛盾しない．設定難易度と普及率の相関については 4.3 節で議論する．

DNS Cookie ルートドメインや TLD では全般に DNS Cookie の普及率は高い傾向にあったが，以下のような留意点がある．ルートドメインの場合，13 個の IP アドレスのうち，B，C，G，I の 4 つのみが DNS Cookie に対応しており，その他の IP アドレスは非対応である．さらに，応答を返した 4 つの IP アドレスの中でも検証失敗を表す BADCOOKIE エラーを正しく返したサーバは `B-Root` サーバのみであった．少なくとも 1 つの IP アドレスが DNS Cookie に対応していたため，表 3 における Root ドメインの DNS Cookies 対応率は 100%となっている．同様に，ccTLD の権威サーバでは，少なくとも 1 つの IP アドレスが DNS Cookie に対応しているドメイン名は 81%以上存在していた一方，1 つのドメイン名に対する IP アドレス間

表 3　DNS セキュリティ機構への対応率

DNS servers	DNSSEC	DNS Cookie	CAA	MX	SPF	DMARC	MTA-STS	DANE	TLSRPT
ROOT	100.00 %	100.00 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %
ccTLD	**56.69** %	**81.10** %	0.00 %	6.30 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %
gTLD	**100.00** %	45.45 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %	0.00 %
Top 10	**0.00** %	20.00 %	30.00 %	90.00 %	100.00 %	88.89 %	33.33 %	0.00 %	33.33 %
Top 100	4.00 %	21.00 %	48.00 %	86.00 %	96.51 %	84.88 %	5.81 %	0.00 %	5.81 %
Top 1K	9.20 %	13.80 %	22.70 %	88.10 %	92.85 %	74.01 %	1.48 %	0.57 %	1.82 %
Top 5K	8.60 %	18.58 %	14.90 %	87.76 %	89.86 %	58.49 %	0.75 %	0.84 %	0.98 %
Top 10K	**7.67** %	17.40 %	12.98 %	86.75 %	88.66 %	54.09 %	0.51 %	0.84 %	0.74 %

で，応答結果が異なっていたドメイン名が 63%程度存在した．これらの事実は，DNS Cookie に対応した主要なドメイン名は多いが，正しく設定されているケースは少ないことを示唆している．

Popular では，DNS Cookie の普及率は 20%程度に留まり，高くない．DNS Cookie は，BIND など，一部の最新版のソフトウェアではデフォルトで有効になるが，Anycast との相性が問題視されていたため，現時点ではまだ普及が進んでいないと考えられる [2]．この問題に対し，RFC9018 [27] が標準化され，サーバ Cookie の新たなフォーマットを定義し，Anycast 利用時でも問題無く設定できるようになった．今後，普及率が上がる可能性がある．

SPF, DMARC, MTA-STS, TLRRPT, DANE 前述したように，これらのセキュリティ機構は，電子メールを運用しているドメイン名が必要とするものである．以下では，電子メールを運用しているケースが多い人気ドメインの方に注目する．

SPF と DMARC は他のセキュリティ機構と比較して，普及率が高いことがわかる．特に上位 100 位以内のドメイン名において，普及率は 80–100%と高い水準にある．一方，MTA-STS，TLSRPT，については上位 10 個のドメイン名における普及率は 33%程度，それよりも下位のドメイン名における普及率は 0–6%程度であった．さらに，DANE については，人気度の高さによらず，1%未満の普及率であった．2021 年現在，これらのセキュリティ機構の普及率が低い水準に留まる理由は，比較的新しい仕様であること，およびそれらのセキュリティ機構を設定するコストが高い点に要因があると考えられる．設定コストと普及率の相関に関しては，4.3 節で議論する．

4.2　DNS セキュリティ機構の共起・依存関係の分析

複数のセキュリティ機構が同時に採用されている（共起）状況や，依存関係を理解することを目的とした分析を行う．このような分析により，採用されやすいセキュリティ機構とそうではないセキュリティ機構の差異を明らかにすることができる．Popular100 個のドメイン名および，上位 5000 位から 5100 位までのドメイン名について，各セキュリティ機構の採用状況を可視化した結果を図 1 に示す．図において，各ドメイン名が採用したセキュリティ機構は黄色で示されている．まず，SPF と DMARC は高い相関を持つことがわかる．この結果は，どちらの機能も採用率が高いことから明らかである．また，上位 20 個のドメイン名では，MTA-STS と TLSRPT は同時に対応される傾向が高いことがみてとれる．最後に，DNSSEC に対応しているドメイン名のほとんどは，全て DNS Cookie にも対応していた．設定が困難である DNSSEC に対応できるドメイン名管理者は，比較的新しい技術である DNS Cookie にも対応できる能力があると推察できる．以下ではより一般的に相関を分析した結果を示す．これ以降の調査は，有効な MX レコードをもつ IP アドレスを対象としている．

図 2 に，セキュリティ機構の共起状況を示す．行と列の交点が，共起スコアを示している．共起スコアは，共起した IP アドレス数の常用対数を取り，最大値を 1 に正規化した数値である．図より，SPF と DMARC，DNS Cookie と SPF，CAA と SPF の共起スコアが高いことがわかる．前述したように SPF，DMARC 自体の対応率が高いため，必然的にこれらの共起スコアも高くなる．後に議論するように，これらのセキュリティ機構は設定コストが低いため，共起しやすいと予想される．

図 3 は，あるドメイン名がセキュリティ機構 X に対応している条件の下で，セキュリティ機構 Y に対応している条件付き確率 $P(Y|X)$ を示す．このように定義した条件付き確率により，機構 Y が X に対してどのような依存性があるかを計測できる．はじめに，MTA-STS を設定したドメイン名は，高い確率で TLSRPT を設定する傾向があることがみてとれる．TLSRPT は，MTA-STS のエラーをレポートする機能であるため，このような結果を得ることは自然であると考えられる．同様に，DANE に対応するドメイン名は，DNSSEC も対応する傾向が高いことが明らかになった．DANE を利用するには DNSSEC が必須事項であるため，このような依存関係が生じたと考えられる．なお，外部のメールサーバを利用し MX レコードに登録することがあるため，依存関係は必ずしも 100%とはならない．このように，機構間には固有の依存関係があることが示された．

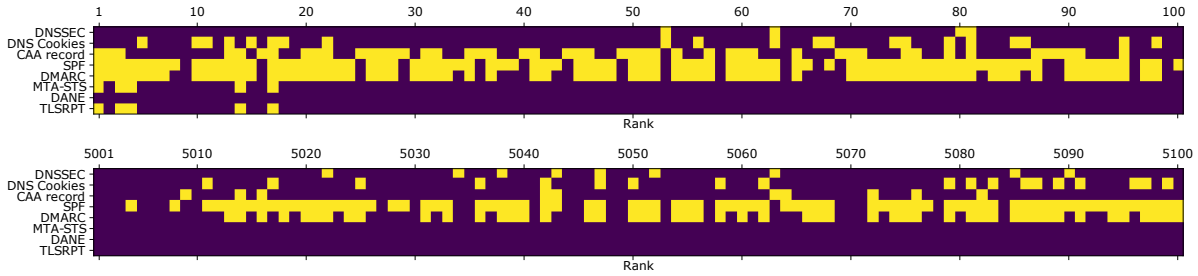

図 1 個々のドメイン名に対する DNS セキュリティ機構の対応．それぞれのドメイン名にて，対応しているセキュリティ機構を黄色で示す．

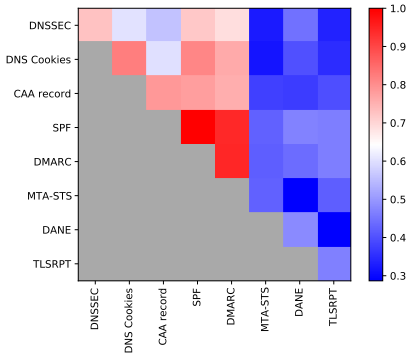

図 2 DNS セキュリティ機構の共起状況

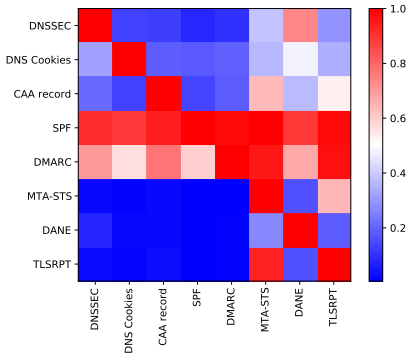

図 3 セキュリティ機構 X に対応している条件の下でセキュリティ機構 Y に対応している条件付確率 $P(Y|X)$

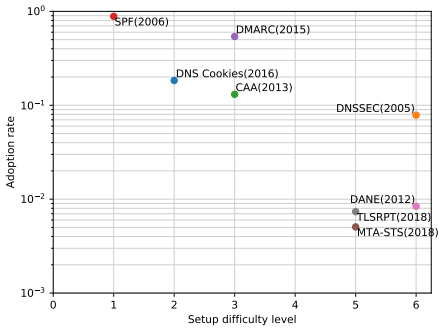

図 4 設定難易度に対する普及率．括弧内の数字は標準化された年を表す．

4.3 設定難易度と設定率の関係

以下では，セキュリティ機構の設定難易度と，設定率の関係を分析する．はじめに，それぞれのセキュリティ機構の設定難易度のスコアを定義する．表 4 に，必要となる設定種別ごとのスコアを示す．DNS リソースレコードの設定はコストが低いため，スコアは最も低い 1 点とする．サーバの設定はリソースレコードよりも高いスコアとし，2 点とする．一般に，サーバの設定 (運用パラメータの追加・変更) には事前の動作確認でコストがかかるため，設定が必要な種類が多いほどスコアを加算する．「第三者の介入」は，単一のリソースレコードやサーバの設定だけでは完結しないケースに相当し，例えば DNSSEC における上位ドメイン名との連携が挙げられる．複数組織による調整，検証が必要なことから，スコアは最も高い 3 点とした．最終的に，セキュリティ機構に必要な設定すべてに対するスコアを加算し，設定難易度のスコアとする．表 5 に各セキュリティ機構の設定難易度スコアを示す．難易度が最も低いのは SPF，最も高いのは DNSSEC，DANE である．

表 4 必要となる設定毎の難易度スコア内訳

No.	設定	スコア
I	リソースレコードの設定を要する	1
II	DNS サーバの設定変更を要する	2
III	メールサーバの設定変更を要する	2
IV	Web サーバの設定変更を要する	2
V	設定に第三者の介入を要する	3

図 4 に，設定難易度と設定率の散布図を示す．SPF の設定率と，他のセキュリティ機構の設定率との差が大きいため，設定率は対数軸とする．また，有効な MX レコードが含まれる IP アドレスのみを対象としている．図 4 からもわかるように，設定難易度が低いほどその機能への設定率は高い．加えて，設定難易度が同等のセキュリティ機構については，より古くから存在する機能の方が，新しい機能よりも設定率が高い傾向にあることが明らかになった．このことは，セキュリティ機構の設定率を高めるために，設定難易度を下げることが重要であることを意味する．

4.4 DNS オペレータの調査

DNS セキュリティ機構の利用状況とその理由をさらに深く分析することを目的として，権威 DNS サーバやフル

表 5　セキュリティ機構の設定難易度スコア

セキュリティ機構	必要な設定					スコア
	I	II	III	IV	V	
SPF	1					1
DNS Cookie		2				2
DMARC	1		2			3
CAA	1			2		3
MTA-STS	1		2	2		5
TLSRPT	1		2	2		5
DNSSEC	1	2			3	6
DANE	1	2			3	6

リゾルバを運用している DNS オペレータを対象に，オンライン調査を実施した．著者らが所属する組織の関係者を対象に，オンライン調査への協力を依頼し，2021 年 8 月 16 日から 8 月 21 日までの 6 日間を調査期間とした．この結果，ISP，学術ネットワーク管理者，組織 IT 部門などに従事する実験協力者から 6 件の回答を得た．なお，収集した情報は匿名化し，統計的に処理した．SPF の設定率は 4/6 であり，高かった．この結果は，図 3 に示す結果とも一致する．一方，その他のセキュリティ機構の設定率はいずれも低く，最大でも 2/6 (DNSSEC 検証)，であり，DKIM，DMARC，MTA-STS，TLSRPT は設定例がなかった．セキュリティ機構を設定していない理由として，「スキル・稼働時間の不足」が 4 件，「需要がない」が 2 件挙げられた．DNSSEC については，「上位のドメイン名が署名を行っていないため設定できない」という意見も存在した．最も意見が多かった「スキル・稼働時間の不足」は，4.3 節で示した，設定難易度が設定率に影響する観察結果と通底する．すなわち，設定に要するコストを下げることで，普及率が向上する余地があることが，オペレータ調査の結果からも示唆される．

5. 議論

5.1 制約事項および今後の展望

本研究では，権威 DNS サーバのセキュリティ機構に焦点を当てた．しかし，スタブリゾルバやフルリゾルバについても，セキュリティ機構は存在する．例えば，DoH や DoT はスタブリゾルバとフルリゾルバ間の通信を暗号化する機能である．加えて，DNSSEC や DNS Cookie は，サーバ側，クライアント側双方が設定を正しく行わなければ上手く機能しない．さらに，QNAME minimization のように，スタブリゾルバのプライバシーを守る機能も存在する．これらのスタブリゾルバ，フルリゾルバに関する DNS セキュリティ機構についても対応割合を調査し，正しく設定が行われているかどうか調べることは，今後の課題である．

本研究が示すように，いくつかの DNS セキュリティ機構は設定率が低い．本研究は，その主要因は設定に要するコストにあると推論した．推論の正当性を検証することを目的として，本研究ではドメイン名管理者に対するオンライン調査を実施した．この結果，推論を支持する結果を得た．しかしながら，調査は一部の組織に偏った小規模なものに留まるため，一般的な知見を得るためには大規模な調査を実施する必要がある．大規模で国際的なオンライン調査の実施は，今後の課題である．

最後に，新しく標準化される DNS セキュリティ機構についても今後の課題として挙げられる．例えば，ESNI [22] は SSL/TLS 暗号化を，DNS レコードに公開鍵を設定することで，今よりもはやく開始できるようにする機能である．Cloudflare のようないくつかのプロバイダは，既に対応を開始している [5].

5.2 DNS セキュリティ機構導入の促進

本研究で分析したセキュリティ機構を適切に設定することにより，DNS のセキュリティレベルを格段に向上させることができる．これらのセキュリティ機構は，いずれも DNS 権威サーバに対して適切に設定を行った上で，必要に応じて Web/メールサーバや TLS ライブラリを適切に設定する必要がある．ドメイン名管理者は，定期的にこれらの機能の設定を見直し，古くなった機能や新しく標準化される機能に対しても対応・削除の検討を行うべきである．

4.3 節で示したように，セキュリティ機構の普及率を高める鍵は，設定のしやすさにあると考えられる．この仮説を裏付ける例として，近年の HTTPS の急速な普及が挙げられる．ウェブサーバの HTTPS 対応が増えた理由は，Let's Encrypt の登場であることがよく知られている [3], [8]. TLS 証明書の生成/インストールや，HTTPS サーバの設定を自動化する無料の証明書やソフトウェアは，HTTPS に対応する障壁を取り除くのに大いに役立っている．さらに，ウェブブラウザは HTTPS による通信をしないウェブサイトに対し，負のセキュリティインジケータを表示するように変化した．このような背景は，ウェブサーバ運用者が積極的に HTTPS 対応をすすめるための動機づけになったと考えられる．上述の HTTPS 普及の成功モデルは，DNS セキュリティ機構の普及を促進する上で大きなヒントになると考えられる．

6. 関連研究

本節では，DNS セキュリティ機構の調査に関する過去の研究について述べる．

Jacob [11] らは，DNS Cookie の大規模な調査を行った．彼らは，DNS Cookie の普及率はサーバ側で 30%以下，クライアント側で 10%以下であること，不正なクエリに特別な処理を行うサーバも少ないことを明らかにした．加えて，サーバ Cookie の分析を行い，時刻同期ができていないサーバや時刻更新が遅いサーバが存在することを示した．

Chung [10] らは，`.com`，`.org`，`.net` の TLD 下にある

DNSSEC 対応ドメイン名に対して，DNSSEC の PKI がどの程度適切に設定されているかを明らかにすることを目的として，21 カ月にわたり大規模な調査を行った．その結果，31 %のドメイン名が DNSSEC に関するレコードを正しく公開ができていないこと，およびた，DNSSEC を要求したリゾルバのうち，実際に正しく検証を行っていたのはわずか 12 %であったことを明らかにした．

Lee [17] らは，メールシステムで普及が進みつつある DANE について，正しく設定されているかを明らかにすることを目的として，24 カ月にわたる大規模な調査を行った．その結果，TLSA レコードの 36 %について，DNSSEC のレコードの不備が原因で検証に失敗すること，および，14 %以上は証明書と矛盾していることを明らかにした．また，DANE をサポートしているメールサービスプロバイダ 4 社のうち 2 社は，TLSA レコードの検証を行っていないことを明らかにした．

上記の研究はいずれも個別の DNS セキュリティ機構に関する調査であった．これらの研究は，いずれのセキュリティ機構も現時点で普及率が低いのみならず，設定にも不備があることがわかる．これらの研究と対照に，本研究は複数の DNS セキュリティ機構を対象とした横断的調査を行った．この結果，セキュリティ機構間の普及率の差異を生み出すいくつかの要因明らかにした．そのような知見は，将来的にセキュリティ機構が普及していくことを促進するのに有益である．

7. 結論

本研究では，主要な DNS セキュリティ機構である DNSSEC, DNS Cookie, CAA, SPF, DMARC, MTA-STS, DANE および TLSRPT の普及率を大規模に調査した．その結果，ルートドメインや TLD など，主要な DNS インフラストラクチャでは，DNSSEC や DNS Cookie の普及率が高いことを明らかにした．また，一般的な登録ドメイン名では，DNS セキュリティ機構の多くは普及率が低い状況にあること，および設定が容易なセキュリティ機構ほど，普及率が高い傾向にあることを明らかにした．セキュリティ機構の普及率向上に向けて，DNS オペレータに対するより大規模なユーザスタディの実施，設定を容易にするソフトウェアの開発，新たな機能の普及率調査，経時的なモニタリングの継続は今後の課題である．

参考文献

[1] : DNS amplification attack, https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/.

[2] : DNS cookies on servers in anycast clusters or behind load balancers, https://kb.isc.org/docs/dns-cookies-on-servers-in-anycast-clusters.

[3] : Let's Encrypt, https://letsencrypt.org/.

[4] : Tranco, https://tranco-list.eu/.

[5] : What is encrypted SNI? — How ESNI works, https://www.cloudflare.com/learning/ssl/what-is-encrypted-sni/.

[6] : Domain names - concepts and facilities, RFC 1034 (1987).

[7] 3rd, D. E. E. and Andrews, M. P.: Domain Name System (DNS) Cookies, RFC 7873 (2016).

[8] Aas, J. et al.: Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web, *Proc. ACM CCS*, p. 2473–2487 (online), DOI: 10.1145/3319535.3363192 (2019).

[9] Barnes, R.: Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE), RFC 6394 (2011).

[10] Chung, T. et al.: A Longitudinal, End-to-End View of the DNSSEC Ecosystem, *Proc. USENIX Security Symposium*, pp. 1307–1322 (2017).

[11] Davis, J. and Deccio, C.: A Peek into the DNS Cookie Jar, *Proc. PAM*, pp. 302–316 (2021).

[12] Hallam-Baker, P., Stradling, R. and Hoffman-Andrews, J.: DNS Certification Authority Authorization (CAA) Resource Record, RFC 8659 (2019).

[13] Hoffman, P. E.: SMTP Service Extension for Secure SMTP over Transport Layer Security, RFC 3207 (2002).

[14] ICANNWiki: Country code top-level domain, https://icannwiki.org/Country_code_top-leve_domain.

[15] Kucherawy, M. et al.: DomainKeys Identified Mail (DKIM) Signatures, RFC 6376 (2011).

[16] Kucherawy, M. and Zwicky, E.: Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC 7489 (2015).

[17] Lee, H. et al.: A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email, *Proc. USENIX Security Symposium*, pp. 613–630 (2020).

[18] Lian, W. et al.: Measuring the Practical Impact of DNSSEC Deployment, *Proc. USENIX Security Symposium*, pp. 573–588 (2013).

[19] Man, K. et al.: DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels, *Proc. ACM CCS*, p. 1337–1350 (online), DOI: 10.1145/3372297.3417280 (2020).

[20] Margolis, D. et al.: SMTP TLS Reporting, RFC 8460 (2018).

[21] Müller, M. et al.: Rolling With Confidence: Managing the Complexity of DNSSEC Operations, *IEEE Transactions on Network and Service Management*, Vol. 16, No. 3, pp. 1199–1211 (online), DOI: 10.1109/TNSM.2019.2916176 (2019).

[22] Rescorla, E. et al.: TLS Encrypted Client Hello, Internet-Draft draft-ietf-tls-esni-10, Internet Engineering Task Force (2021).

[23] Rose, S. et al.: DNS Security Introduction and Requirements, RFC 4033 (2005).

[24] Rose, S. et al.: Protocol Modifications for the DNS Security Extensions, RFC 4035 (2005).

[25] Rose, S. et al.: Resource Records for the DNS Security Extensions, RFC 4034 (2005).

[26] Schlitt, W. and Wong, M. W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, RFC 4408 (2006).

[27] Surý, O. et al.: Interoperable Domain Name System (DNS) Server Cookies, RFC 9018 (2021).

[28] 矢島ほか：DNS Cookie の普及・運用状況の実態調査と今後の展望，信学技報 (ICSS2020-28) (2021).