DNSセキュリティ機構の普及状況調査：現状と今後の課題

DNS Summer Day 2022

矢島雅紀（早稲田大学） 千葉大紀（NTT） 米谷嘉朗（日本レジストリサービス）

森 達哉（早稲田大学/NICT）

概要

目的

- 主要なDNSセキュリティ機構について大規模な実態調査を実施
  - DNSSEC, DNS Cookie, CAA, SPF, DMARC, MTA-STS, DANE,TLS-RPT

結果

- 主要なDNSインフラストラクチャでは普及率が高い
- 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

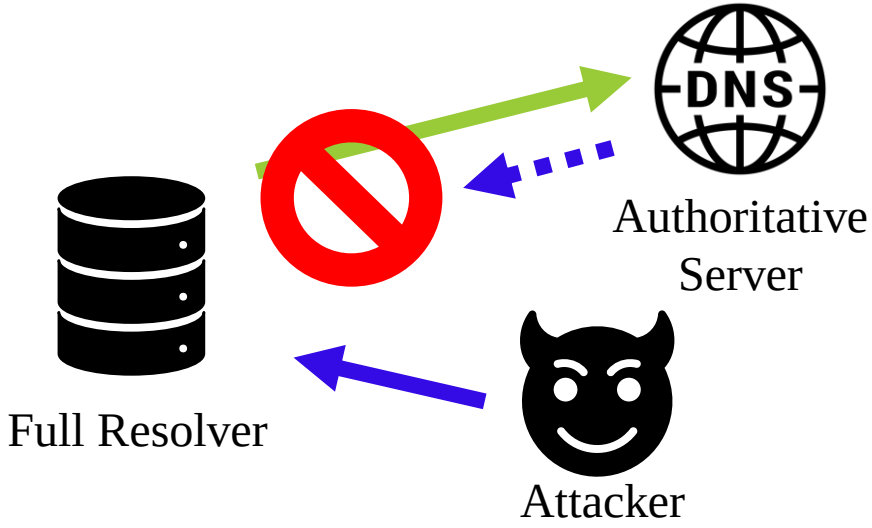
DNSセキュリティ機構

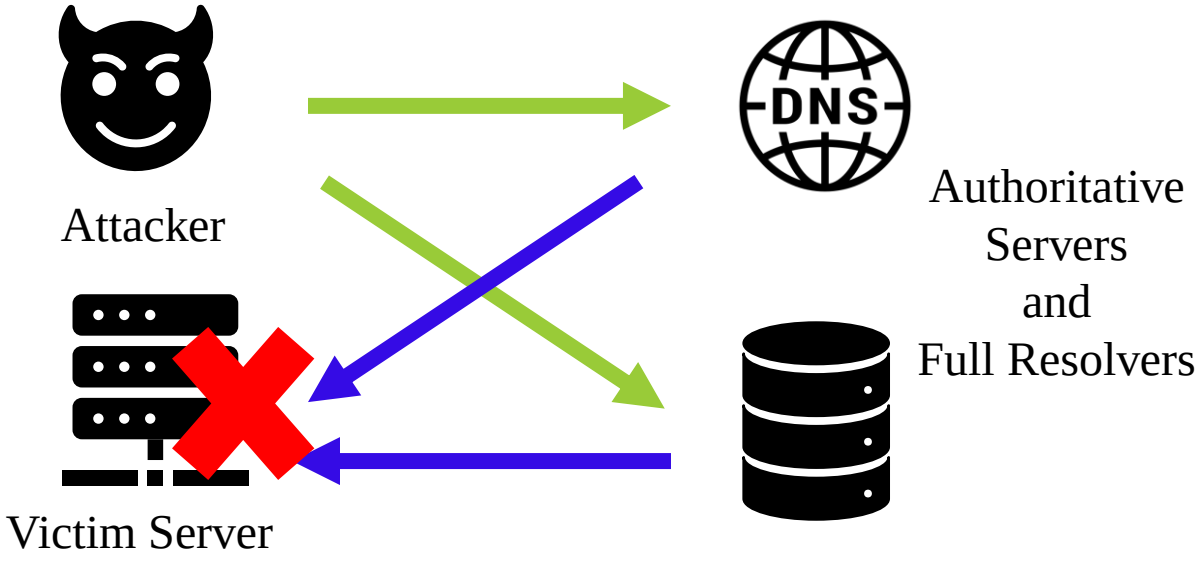
- DNSを標的としたセキュリティ脅威は、以下の3つに分類できる:
  - DNSサーバを対象とした脅威
    (DNSキャッシュポイズニング攻撃、DNS アンプ攻撃)
  - DNSが扱う名前を対象とした脅威
    (偽のドメイン名を用いたフィッシングサイトやマルウェア配布サイト)
  - DNSクエリ情報に含まれるプライバシー情報の漏洩

DNSセキュリティ機構

- DNSサーバを対象とした脅威
  - (DNSキャッシュポイズニング攻撃、DNS アンプ攻撃)

- DNSSEC, DNS Cookie

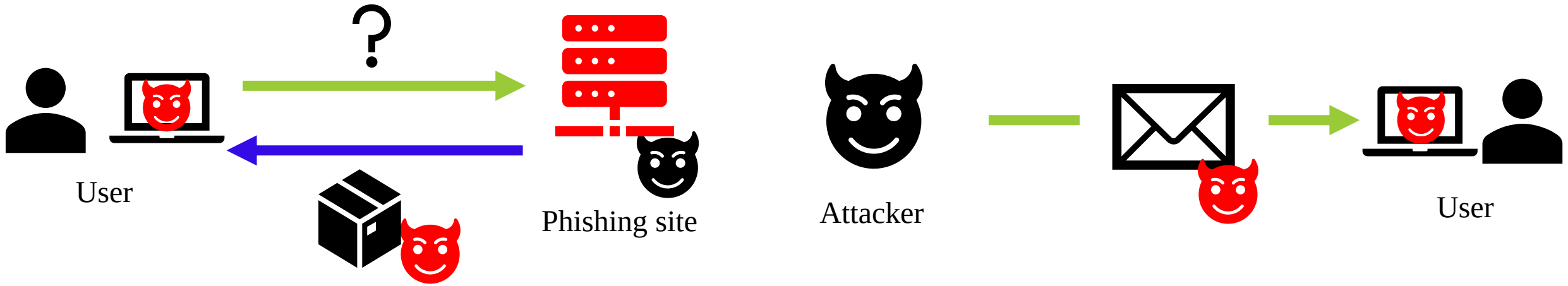




DNSセキュリティ機構

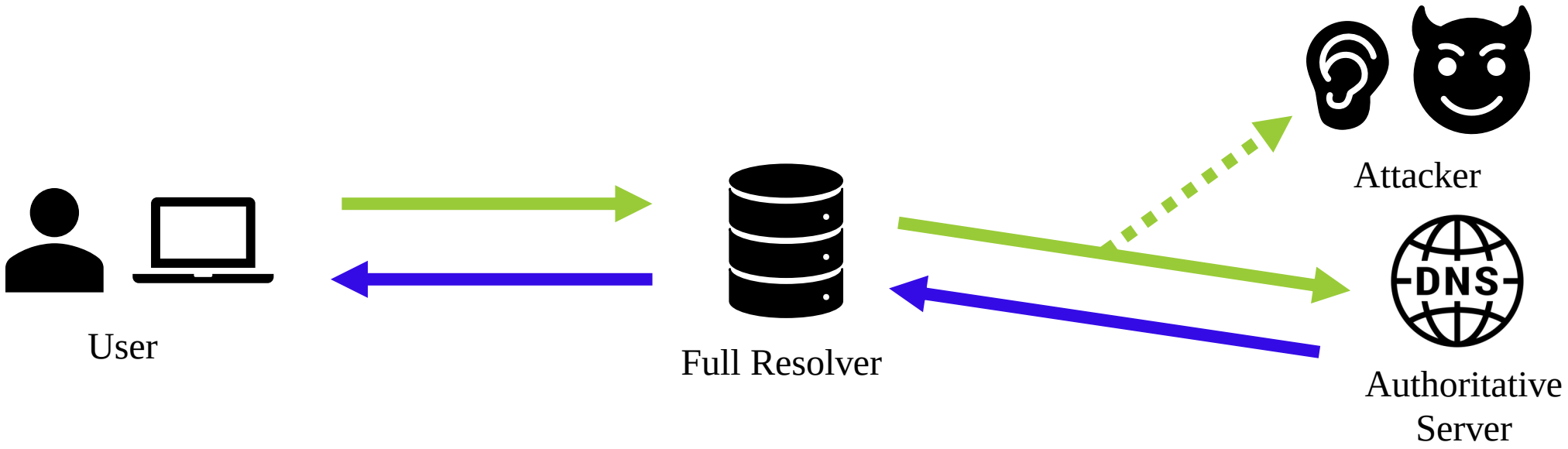
- DNSが扱う名前を対象とした脅威
  - (偽のドメイン名を用いたフィッシングサイトやマルウェア配布サイト)

- CAA, SPF, DMARC, MTA-STS, DANE, TLSRPT



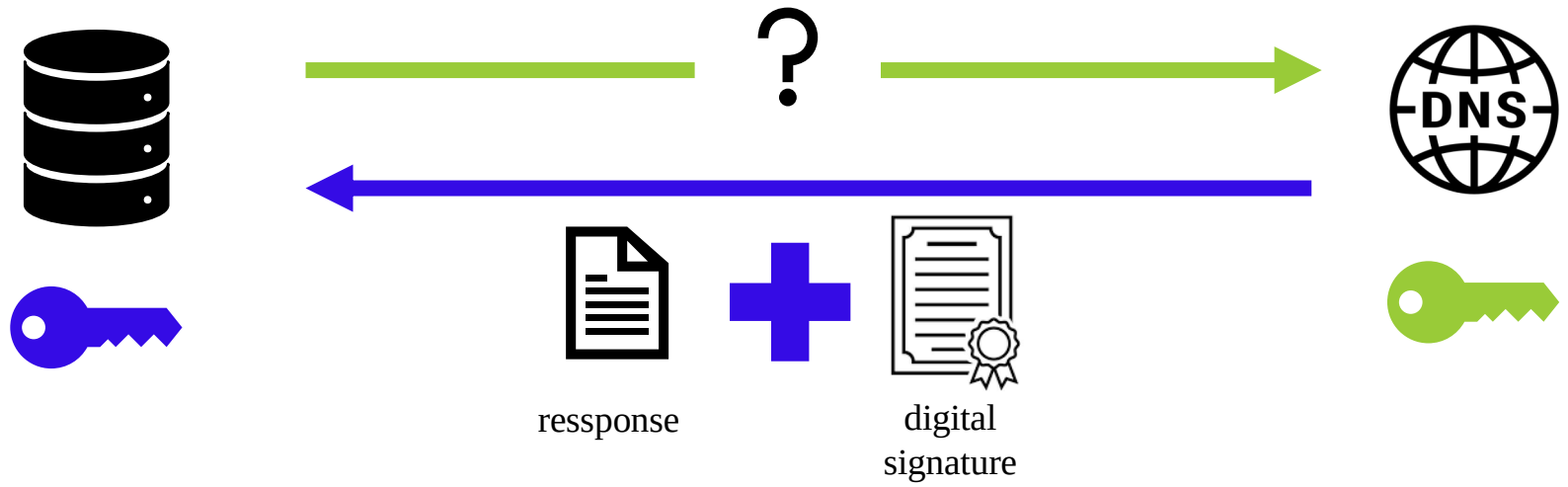
DNSセキュリティ機構

- DNSクエリ情報に含まれるプライバシー情報の漏洩
- DNS over TLS(DoT), DNS over HTTPS(DoH), …



DNSSEC

- DNSSECは、DNS応答の完全性を保証するメカニズム
  - 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

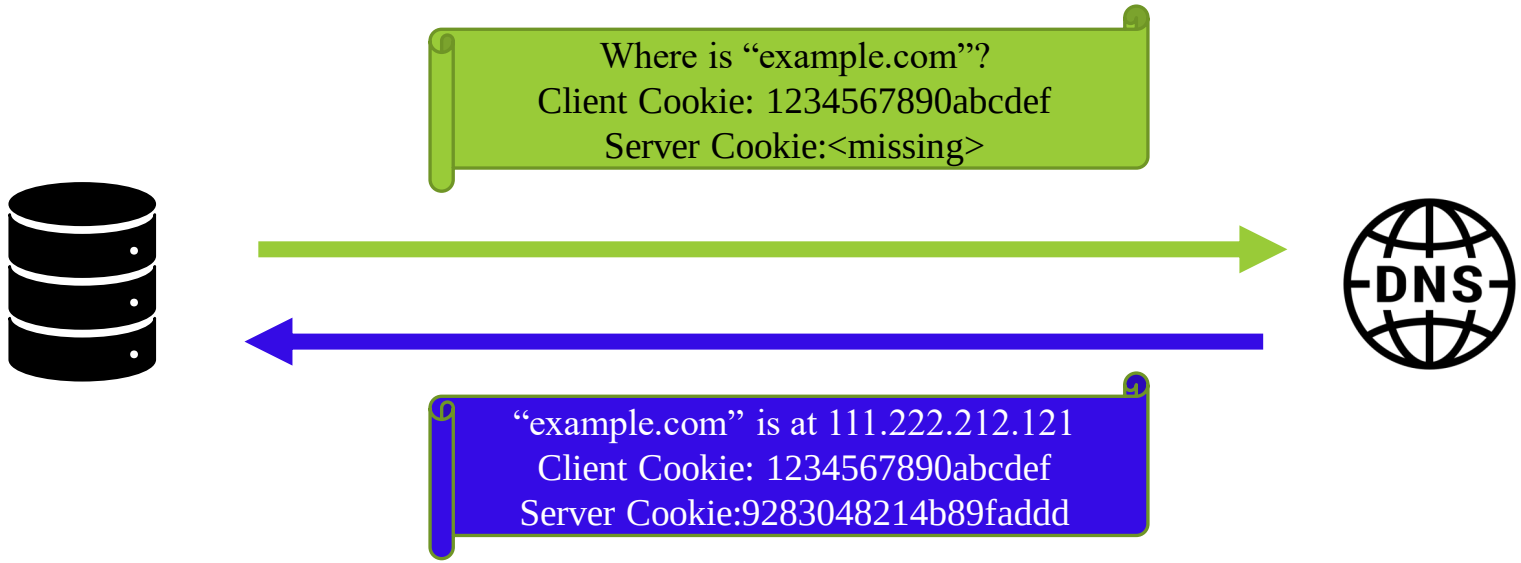


DNSSEC

- DNSSECはあくまで応答の完全性のみ保証する
  - 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
- DNSSECを有効化するには、ゾーン管理者が積極的に対応する必要がある

DNS Cookie

- 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
  - クライアントとサーバはそれぞれがDNS Cookieを検証する



DNS Cookie

- 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
- DNS Cookieへの対応難易度は、DNSソフトウェアの実装やデフォルト設定に依存する

CAA

- 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

- 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

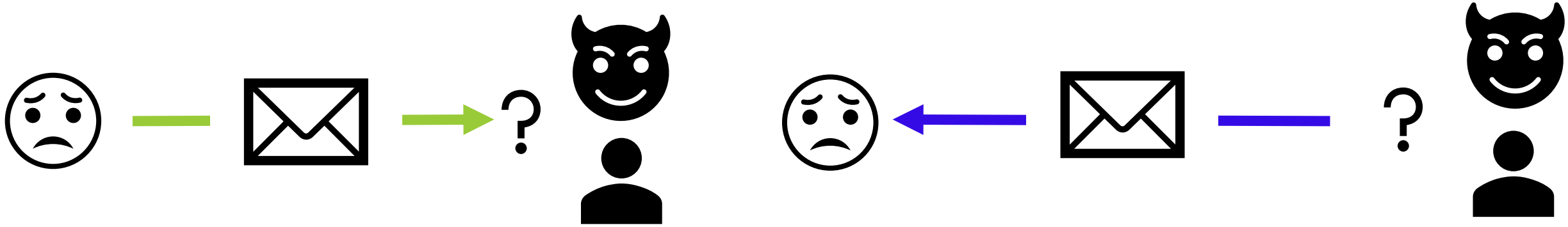
```
;; ANSWER SECTION:
example.com.            300     IN      CAA     0 issue "example2.com"
example.com.            300     IN      CAA     0 issuewild ";"
example.com.            300     IN      CAA     0 iodef "mailto:info@example.com"
```

Example of CAA RR

Mailに関するセキュリティ機構

- 電子メールの利用時におけるセキュリティを強化するために、様々なセキュリティ機構が存在する
  - SPF, DMARC, MTA-STS, DANE, and TLSRPT

- これらのセキュリティ機構は、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を軽減する



Mailに関するセキュリティ機構

- DMARC および DANEの利用において、
  DNSSEC署名が強く推奨されている

- Mailに関するセキュリティ機構は以下の表の判定指標となる:

Mechanisms	判定指標
SPF, DMARC	メールの送信者認証を有効化しているか
MTA-STS, TLSRPT	メール配送の暗号化の指示と、 そのダウングレードの報告を実施しているか
DANE(TLSA)	HTTPS以外の通信で使用するサーバ証明書 公開鍵を安全に配布しているか

DNSセキュリティ機構

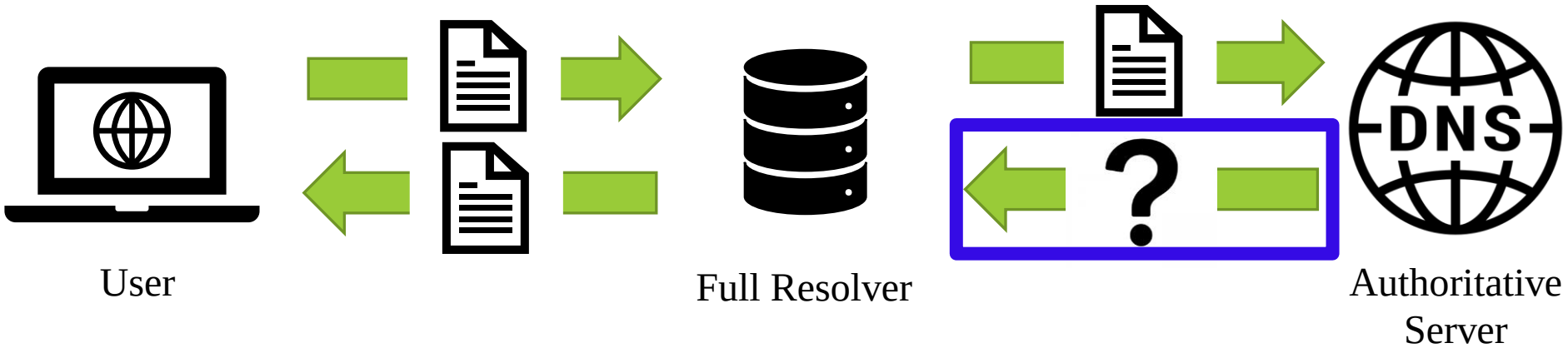
- DNSセキュリティ機構の利用には、DNS RRを設定する必要がある

Table: 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

	Configure	設定するドメイン名	RR	シグネチャ
DNSSEC	Server	<domain name>	RRSIG(, etc)	n/a
DNS Cookies	Server	n/a	n/a	n/a
CAA	Server	<domain name>	CAA	n/a
SPF	Server	<domain name>	TXT	v=spf1…
DMARC	Receiver	_dmarc.<domain name>	TXT	v=DMARC1…
MTA-STS	Receiver	_mta-sts.<domain name>	TXT	v=STSv1…
DANE	Receiver	_25._tcp.<mail domain name>	TLSA	n/a
TLSRPT	Receiver	_smtp._tls.<domain name>	TXT	v=TLSRPTv1…

調査手法

- 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
- 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



データセット

- 本研究では，IPv4のみに着目する

Table:収集したドメイン名とIPアドレスの数

データセット	ドメイン名	IPアドレス
Root	1	13
(legacy) gTLD	22	110
ccTLD	254	993
Popular (Tranco List)	9,999	12,318

結果 – DNSのコア

- DNSサーバ対する脅威への対策となるセキュリティ機構は、DNSの基幹に関わるサーバでの普及率が高い

DNS Servers	DNSSEC[%]	DNS Cookies[%]	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

結果 – 人気ドメイン名

- ウェブで利用されるドメイン名では高くとも2割程度

DNS Servers	DNSSEC[%]	DNS Cookies[%]	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

結果 – メールのセキュリティ機構(1)

- 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

DNS Servers	DNSSEC[%]	DNS Cookies[%]	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

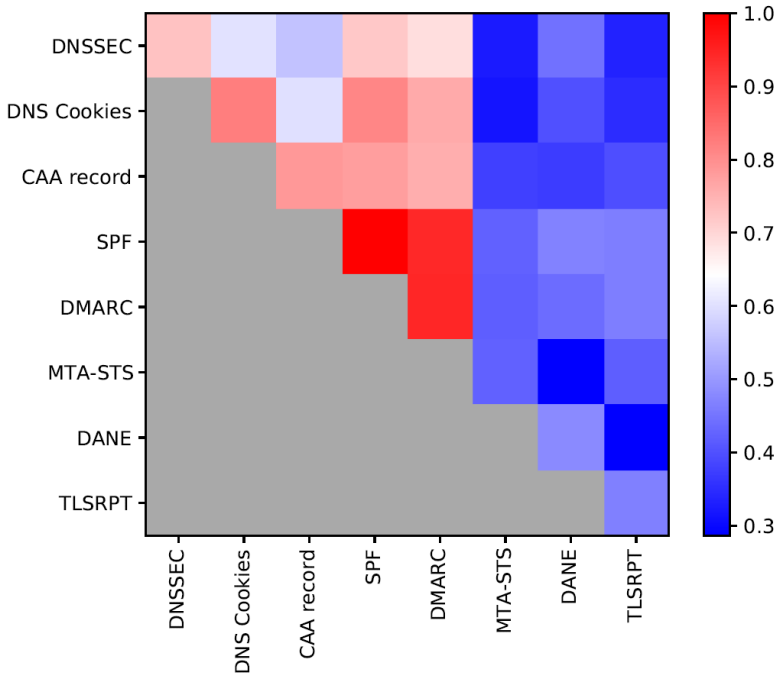
結果 – メールのセキュリティ機構(2)

- DANEについては，人気度の高さによらず、1%未満

DNS Servers	DNSSEC[%]	DNS Cookies[%]	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

結果 – 共起スコア

- DMARC とSPF 、DNS CookieとSPF、CAAとSPFの共起スコアが高い



結果 – 設定難易度と設定率(1)

- 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
- 必要となる設定種別ごとのスコアを定義する:

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

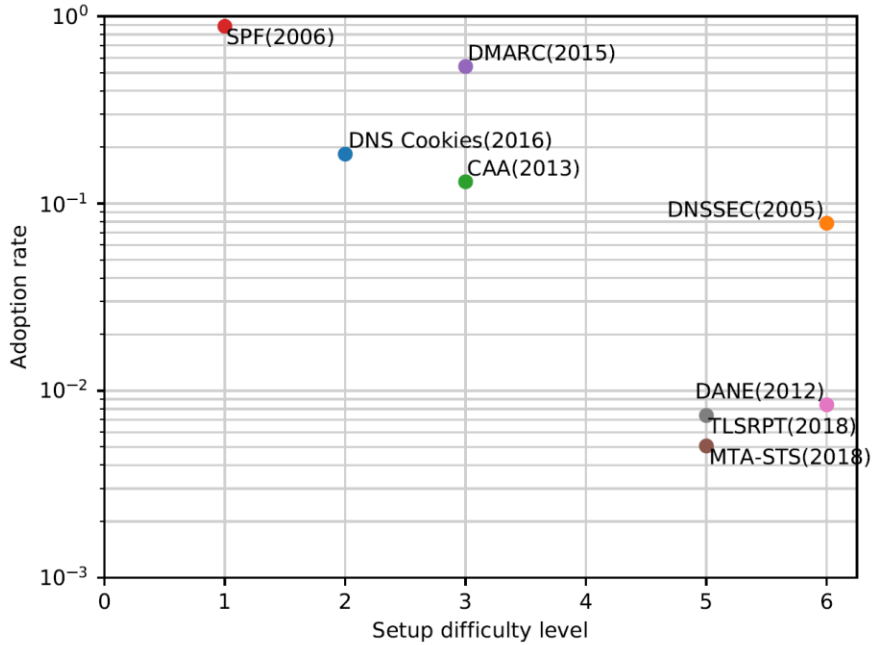
結果 – 設定難易度と設定率(2)

- 最終的な設定難易度のスコアは次のようになる:

セキュリティ機構	必要な設定					スコア
	1	2	3	4	5	
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

結果 – 設定難易度と設定率(3)

- 設定難易度が低いほどその機能の設定率は高い
  - 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



アンケート調査

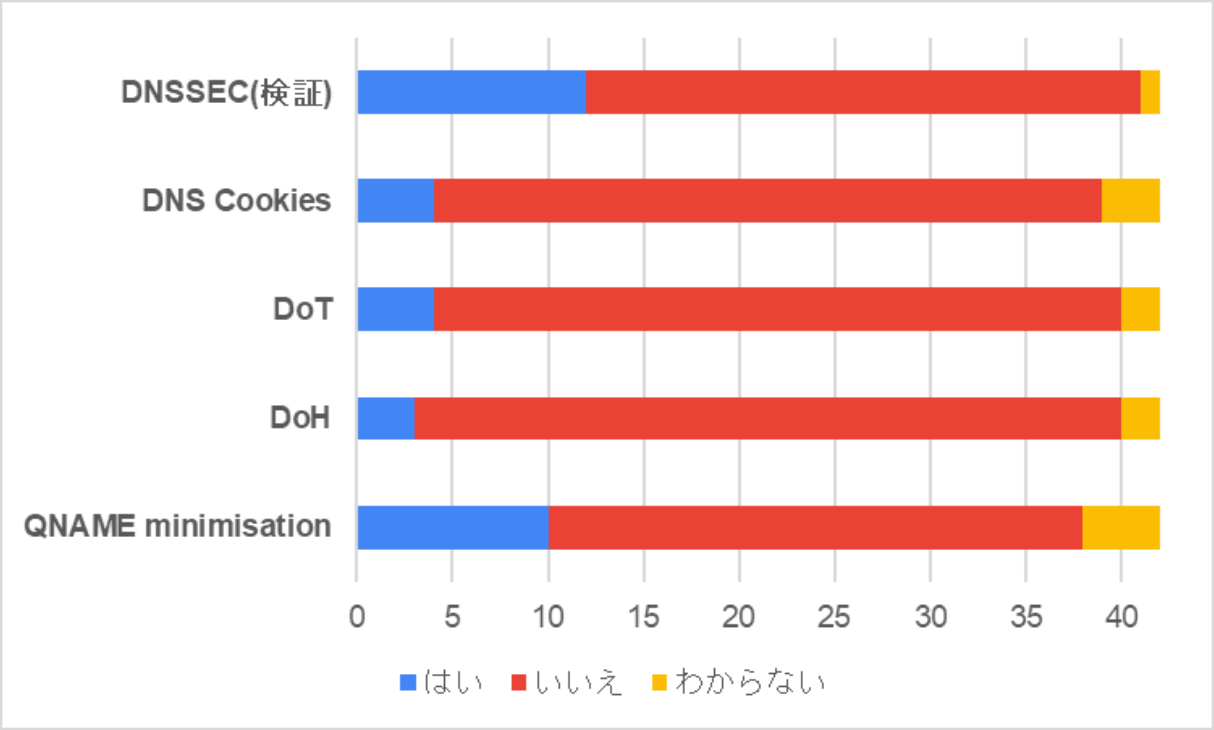
- DNSOPS.JPのメーリングリストにて、アンケートを実施
- DNSサーバに対する調査の裏付け、
  また実際に運用している方々の生の意見を聞く

調査内容

- サーバの種類ごとに、対応しているセキュリティメカニズム、対応していない理由を調査
  - フルリゾルバ:
    - DNSSEC(検証), DNS Cookies, DoT, DoH, QNAME minimization
  - 権威DNSサーバ:
    - DNSSEC(署名), DNS Cookies
  - Webサーバ:
    - サーバ証明書, CAA, AAAA, HTTPS, TLSA
  - メールサーバ:
    - SPF, DKIM, DMARC, MTA-STS, TLSA, TLSRPT, BIMI

フルリゾルバ

- 運用している/していたと回答:42



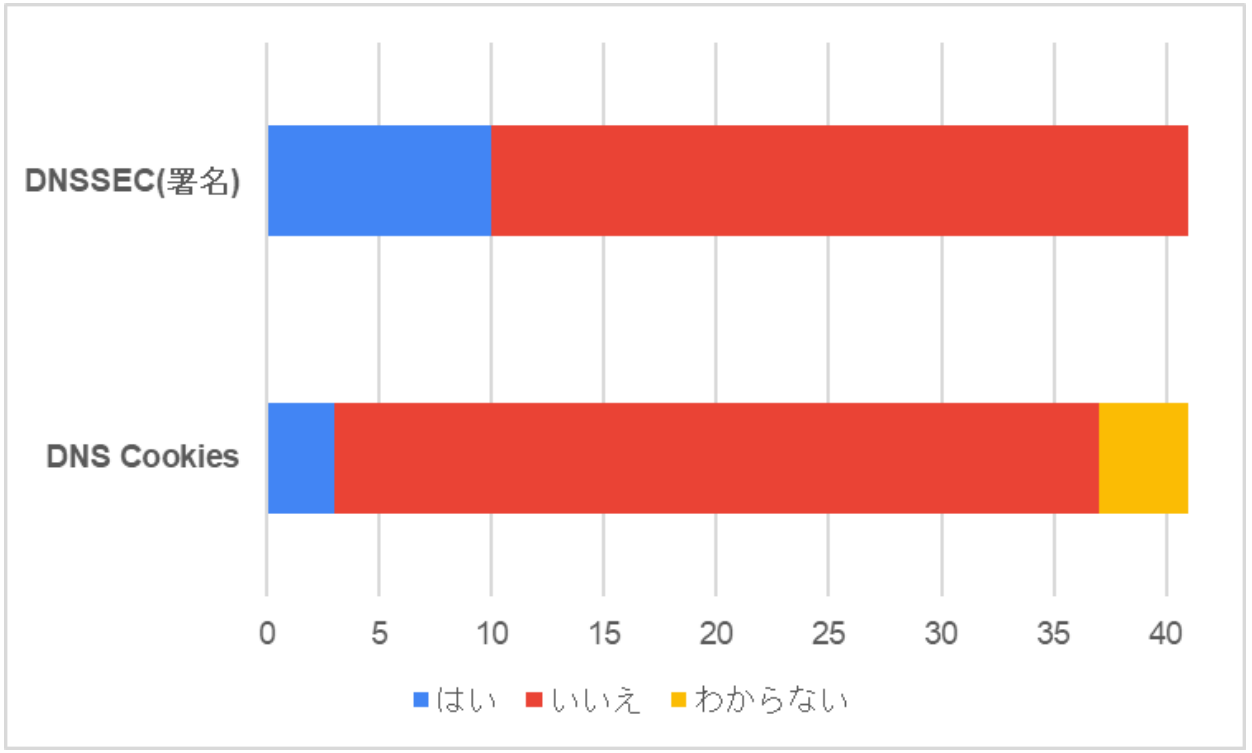
フルリゾルバ

- 設定していない主な理由
  - 運用上特に必要ないから:19
  - 準備不足:9

- その他の理由
  - serv failの際利用者の理解が得難い
  - 8.8.8.8などのpublic DNSで名前解決できて自社のDNSで名前解決できない時に、権威DNSの不備であってもこちらの不備とみなされる
  - unboundは勝手にonにしないから(DNS Cookies)

権威DNSサーバ

- 運用している/していたと回答:41



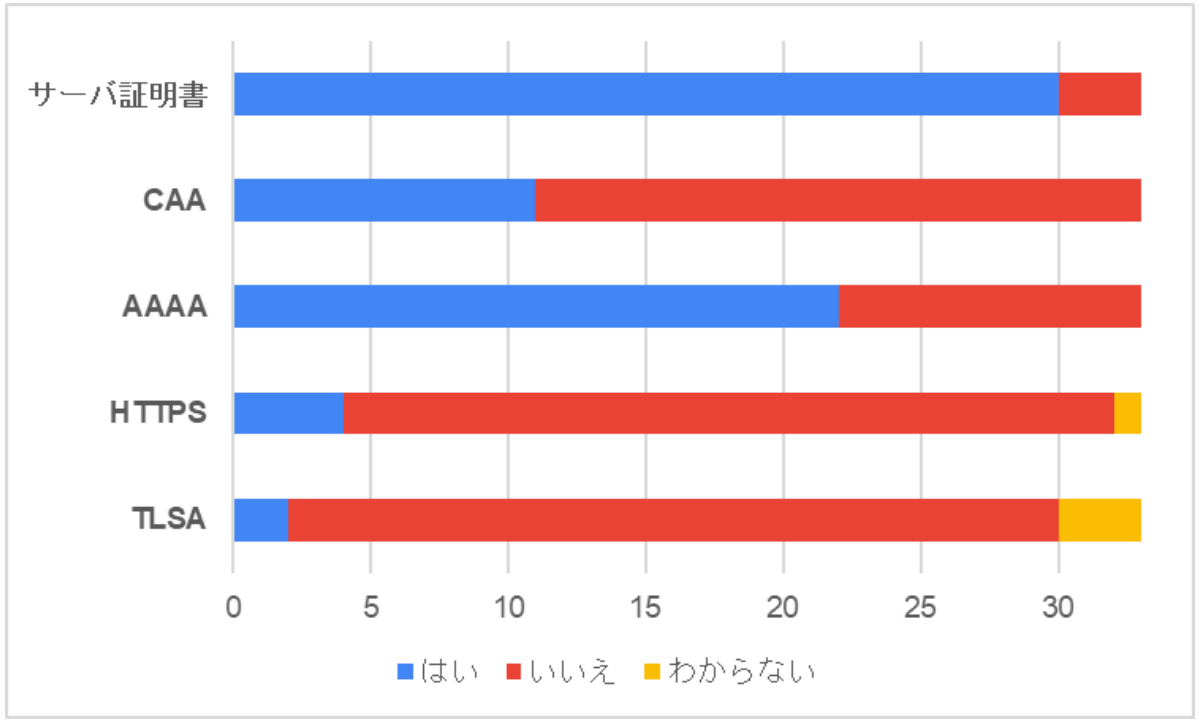
権威DNSサーバ

- 設定していない主な理由
  - 運用上特に必要ないから:17
  - 準備不足:11
  - 利用しているサービスや上位ドメイン名が対応していないため:3
  - 構成上設定するのが難しいため:4

- その他の理由
  - 脆弱性回避のため
  - 名前解決できない場合のほうがセキュリティ上の課題より重要

Webサーバ

- 運用している/していたと回答:33



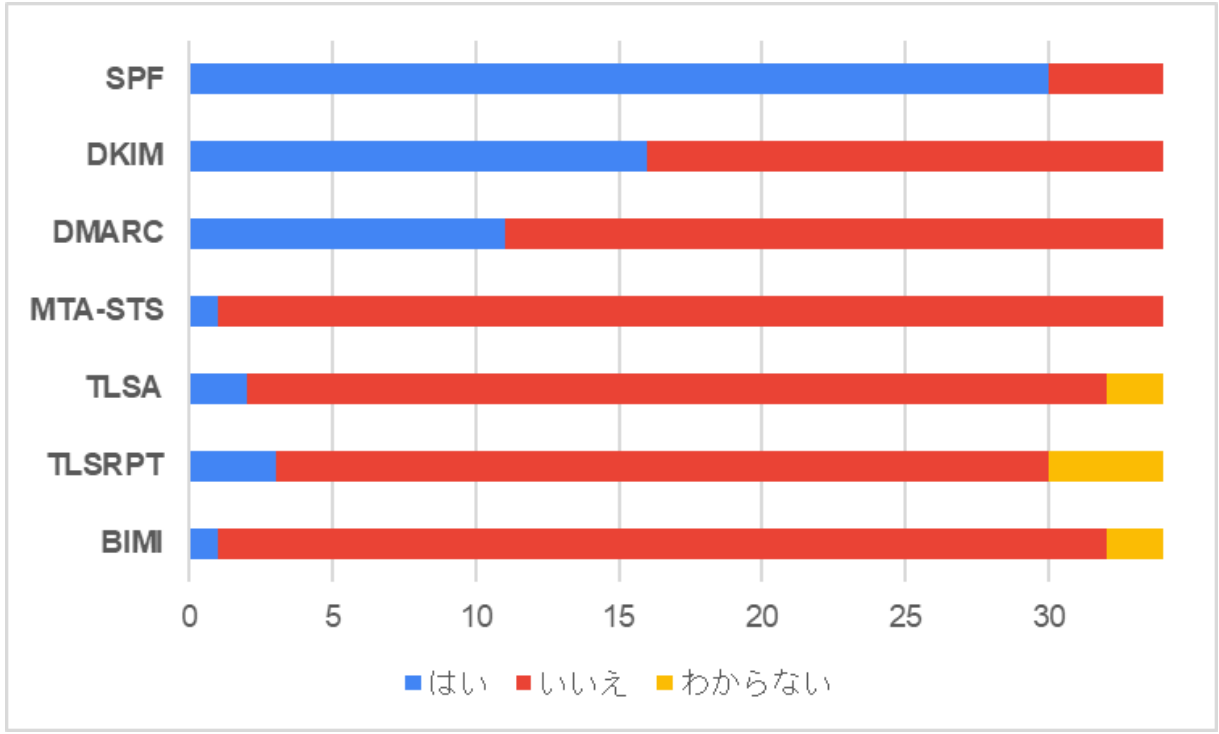
Webサーバ

- 設定していない主な理由
  - 運用上特に必要ないから:22
  - 準備不足:8
  - 利用しているサービスや上位ドメイン名が対応していないため:3
  - 構成上設定するのが難しいため:3

- その他の理由
  - HTTPSレコードはドラフトだから

メールサーバ

- 運用している/していたと回答:34



メールサーバ

- 設定していない主な理由
  - 運用上特に必要ないから:17
  - 準備不足:13
  - 利用しているサービスや上位ドメイン名が対応していないため:2
  - 構成上設定するのが難しいため:7

- その他の理由
  - 電子メールに高度なセキュリティを求めるのが間違い (相手がある話だし)
  - 使用することでより利用者に脅威が発生するため

議論 - サーバに対する調査

- 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
- 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すべきである
- 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

議論 - アンケート調査

- 準備不足や環境の問題でセキュリティメカニズムを設定できないという回答が一定数存在
  - 前述の通り、設定のしやすさを改善することで対応率向上が見込める

- 一方で、それ以外にも様々な理由が存在するため、一概に普及させればいいという問題ではない
  - セキュリティメカニズムそのものの必要性、
  - 対応したがゆえに生じるリスク、
  - サービスとしての可用性

今後の展望

- より大規模なユーザスタディ
  - 世界規模での実施
- 新しく標準化されるDNSセキュリティ機構の実態調査
  (ex:ESNI, BIMI…)
- スタブリゾルバやフルリゾルバ間で機能するセキュリティ機構の実態調査
  (ex:DNSSEC, DNS Cookies…)

まとめ

- DNSセキュリティ機構の普及率を大規模に調査
  - DNSSEC, DNS Cookie, CAA, SPF, DMARC, MTA-STS, DANE, and TLSRPT
- 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
- 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

ご清聴ありがとうございました

Masanori Yajima

y-masa22@nsl.cs.waseda.ac.jp