# ドメイン名をまもるということ

木村泰司

# 概要

- なりすましメールやWebのサーバが本物かどうかを判別するためにユーザが目にするドメイン名。その正しさは、**よくよく注意して確認されるべきと云われるわりに、まぎらわしいドメイン名を使うこと**や、正しいDNS応答かどうかをチェックする**仕組みを導入しないこと**に対して、私たちは**寛容になりすぎて**いないでしょうか。
- DNSは、アドレスシステムが、**コンピューターではなく人にとって分かりやすく運用しやすいものであるために作られたはず**です。分かりにくさ故にユーザが騙されやすくなってしまう環境を変えていくために、私たちができることを、この夏、みなさまに問いかけます。

フィッシング対策協議会
Council of Anti-Phishing Japan

:: フィッシングの報告 :: よくあるご質問 :: お問い合わせ :: コンテンツ利用について

サイト内を検索 検索

ニュース | 報告書類 | 消費者の皆様へ | サービス事業者の皆様へ | フィッシング対策協議会について

HOME > ニュース > 緊急情報

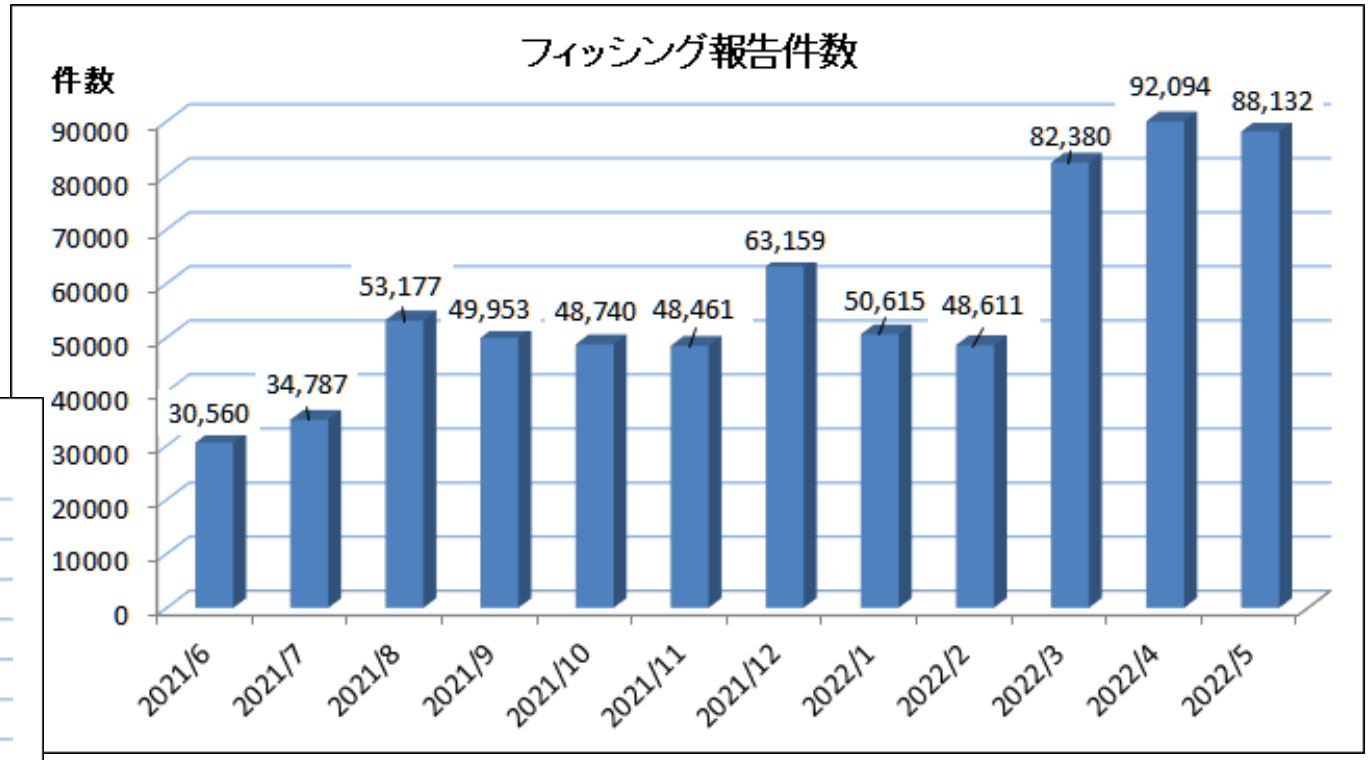
## :: フィッシングに関するニュース

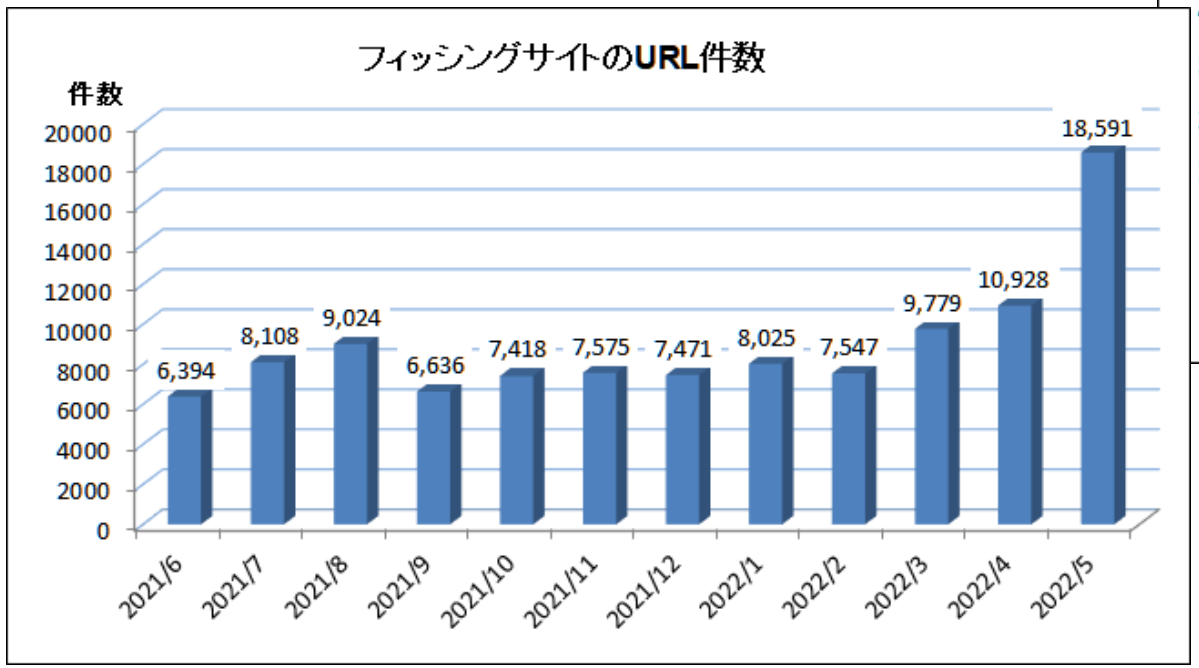
選択してください。
2022年05月19日 住信SBIネット銀行をかたるフィッシング (2022/05/19)
2022年05月06日 フィッシング対策協議会をかたるフィッシング (2022/05/06)
2022年04月25日 @nifty をかたるフィッシング (2022/04/25)
2022年04月19日 NHK をかたるフィッシング (2022/04/19)
2022年04月18日 日本年金機構 (ねんきんネット) をかたるフィッシング (2022/04/18)
2022年04月18日 So-net をかたるフィッシング (2022/04/18)
2022年04月15日 ZOZOTOWN をかたるフィッシング (2022/04/15)
2022年04月15日 mixi をかたるフィッシング (2022/04/15)
2022年04月13日 厚生労働省 (コロナワクチンナビ) をかたるフィッシング (2022/04/13)
2022年04月12日 au をかたるフィッシング (2022/04/12)
2022年04月12日 au をかたるフィッシング (2022/04/12)
2022年03月30日 FamiPay をかたるフィッシング (2022/03/30)
2022年03月25日 出前館をかたるフィッシング (2022/03/25)
2022年03月22日 JR東日本 (モバイルSuica) をかたるフィッシング (2022/03/22)
2022年03月18日 JR西日本をかたるフィッシング (2022/03/18)
2022年03月04日 えきねっとをかたるフィッシング (2022/03/04)
2022年03月04日 千葉銀行をかたるフィッシング (2022/03/04)
2022年02月18日 Yahoo! JAPANをかたるフィッシング (2022/02/18)
2022年02月10日 NTTドコモをかたるフィッシング (2022/02/10)

選択してください。

フィッシング対策協議会　Council of Anti-Phishing Japan | ニュース | 緊急情報
https://www.antiphishing.jp/news/alert/

# フィッシング対策協議会 月次レポートより




フィッシング対策協議会　Council of Anti-Phishing Japan | 報告書類 | 月次報告書 | 2022/05 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202205.html

# 紛らわしいドメイン名

- 他社のドメイン名だが本来のサイトらしいドメイン名
  - submit.example.com
- 前後に文字列を加えたり入れ替えたりしたドメイン名
  - finance.example.com、 www.example.finance.**
- “一見、正規ドメインと見間違えるようなドメイン名”
  - ✓mとrn → micro > rnicro
  - ✓wwとv → will > vvill
  - ✓tとf → soft > soff
  - ：

  (迷惑メール白書2021より)

# わかりやすいドメイン名を使ったとしても…

- **MyEtherWallet.comの事例 - 偽のサーバにアクセスさせて不正送金のスクリプトを実行させ、総額15万ドル（約1630万円）相当が不正送金される。**

**手法**

- **BGP経路(/23など)を/24で経路広告**
- **DNS問い合わせに対して偽のDNSサーバが偽のAレコードを応答**
- **サーバ証明書は自己署名証明書（本来はEV SSL証明書）**

(情報源)
- MyEtherWallet、DNSサーバーにハッキング、15万ドル分のETH盗難か
  https://jp.cointelegraph.com/news/myetherwallet-warns-that-a-couple-of-its-dns-servers-have-been-hacked
- AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet - The Register, 2018/4/24
  https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

# 対策技術(DNSSEC送信メールドメイン認証技術, Webサーバ認証技術)のカバー範囲と特徴 (1/2)

| | 1.メール送信ドメイン認証技術の結果 | 2.メールアドレスのドメイン名 | 3.DNSSECの効果 | 4.Webサイトのドメイン名 | 5.Webサーバ認証技術の結果 |
|---|---|---|---|---|---|
| A.フィッシングではないケース | • 配送される。<br>• (正しさの表示) 安心マーク, BIMI... | • 正しいドメイン名が表示されている。 | • 検証に成功しWebサイトに接続できる。 | • 正しいドメイン名が表示されている。 | • サーバ認証に成功する。 |
| B.メールアドレスドメイン名が紛らわしい＋サイトのURLが紛らわしい | • 配送される。 | • メールのドメイン名が紛らわしく、正しいかどうかの判断がつきにくい。 | • 検証に成功しWebサイトに接続できる。 | • 正しいサイトかどうかの判断がつきにくい。 | • サーバ認証に成功する。 |
| C.メールサーバの詐称＋サイトのURLが紛らわしい | • “reject” → 配送されない。<br>• “none” → 配送される。 | • (配送された場合) 正しいドメイン名が表示されている。 | • 検証に成功しWebサイトに接続できる。 | • 正しいサイトかどうかの判断がつきにくい。 | • サーバ認証に成功する。 |
| D.メールサーバの詐称＋サイトのドメイン名乗っ取り | • “reject” → 配送されない。<br>• “none” → 配送される。 | • (配送された場合) 正しいドメイン名が表示されている。 | • 検証に失敗し、Webサイトに接続できない。 | • 接続できない。 | • 接続できない。 |

枠Y-1　枠Y-2　枠Z　枠X

フィッシングレポート 2022, フィッシング対策協議会 技術・制度検討ワーキンググループ より
https://www.antiphishing.jp/report/phishing_report_2022.pdf

# 送信ドメイン認証技術と DNSSEC が導入されるとエンドユーザーの体験はどう変わるのか

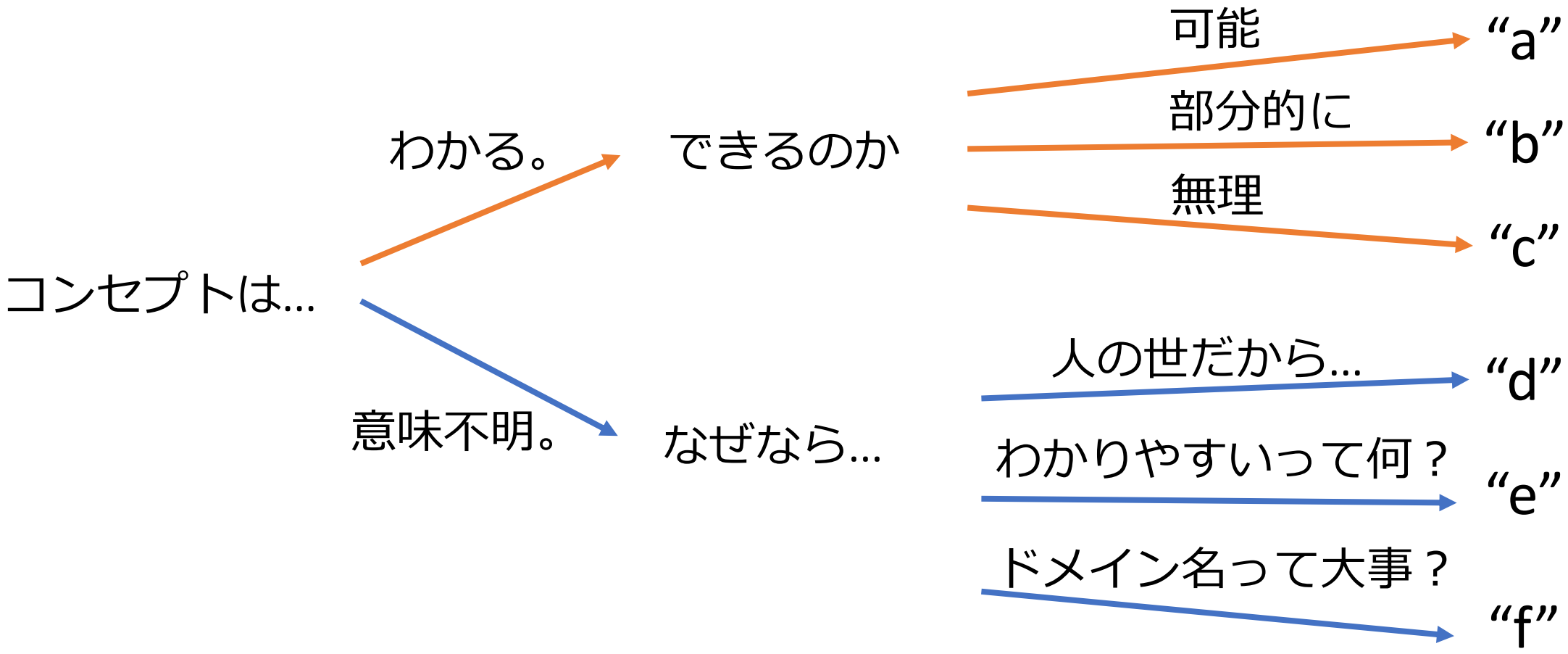
- DMARC の検証ポリシーを reject にすると、ユーザーは紛らわしいドメイン名を判別しなくて良くなる（表中の枠 X）。ただし、DMARC の検証ポリシーが none であるとメールサーバーの管理者が検知できるだけで、ユーザーに起きることは送信ドメイン認証技術の導入前と変わらない。
- メールアドレスに紛らわしいドメイン名が使われると、ユーザーがフィッシングかどうかを判断するにはドメイン名が正しいかどうかを判別する必要がある（枠 Y1）。Web サイトのドメイン名についても同様であ る（枠 Y2）。ユーザーにとってドメイン名が紛らわしいということ自体の判定は難しい。
- DNSSEC の検証で失敗し接続できなくなる挙動は、フィッシングサイト へのアクセスを抑止するという意味ではユーザーを保護する。しかしアクセスできない理由が分からなければユーザーは何とかしてアクセス しようとしてしまうかも知れない。これについては改善の方向性があ る。IETF の RFC8914 に記載されている Extended DNS Error（拡張 DNS エラー）や、提案中の DNS Access Denied Error Page（DNS アクセス禁止に関するエラーページ）である。これらのエラーを受け た Web ブラウザーの表示がどうなっていくのかが注目される。

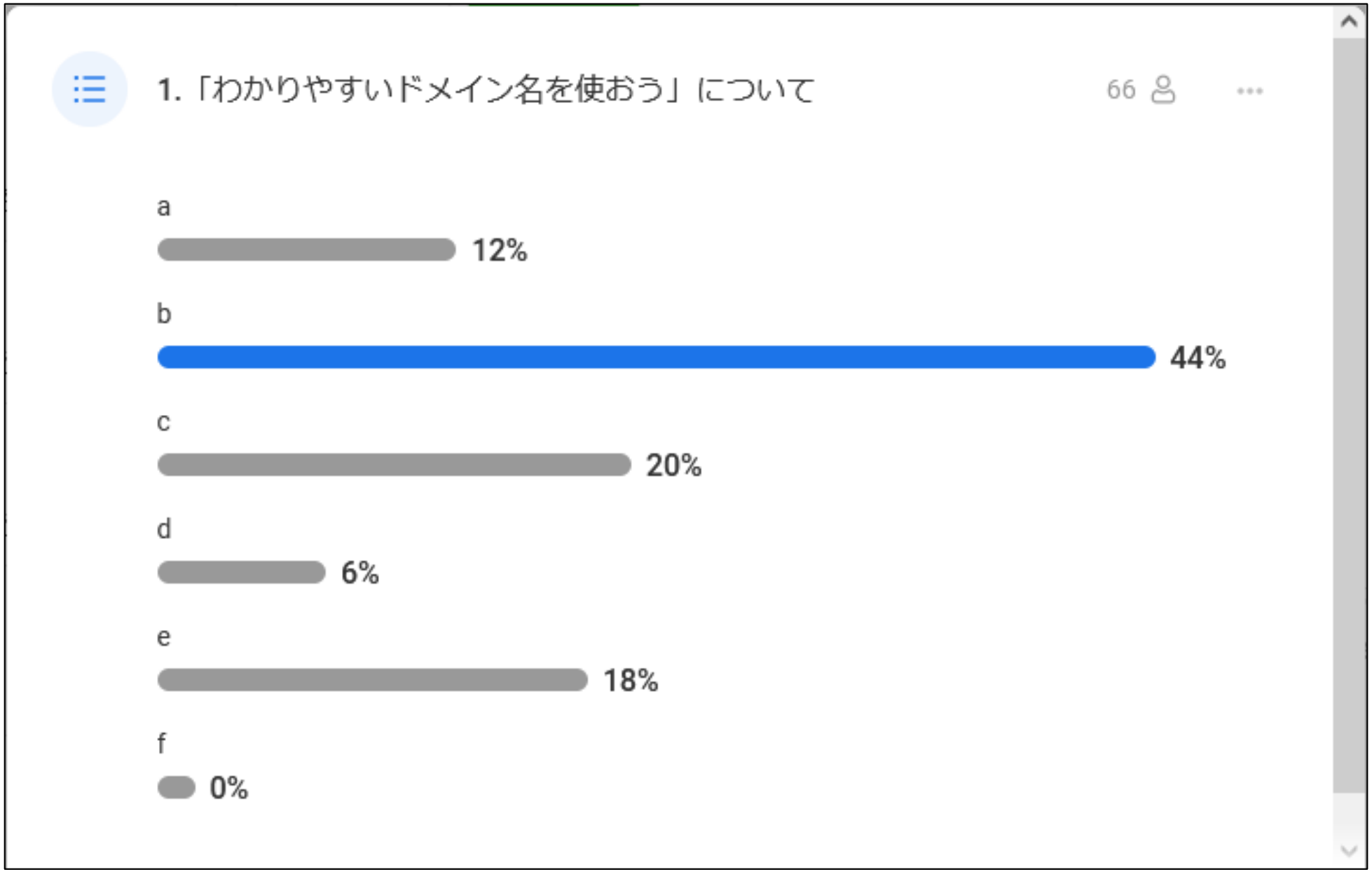
フィッシングレポート 2022, フィッシング対策協議会 技術・制度検討ワーキンググループ より
https://www.antiphishing.jp/report/phishing_report_2022.pdf

# みなさまに問いかけます。

2022年　夏

# 1.「わかりやすいドメイン名を使おう」について





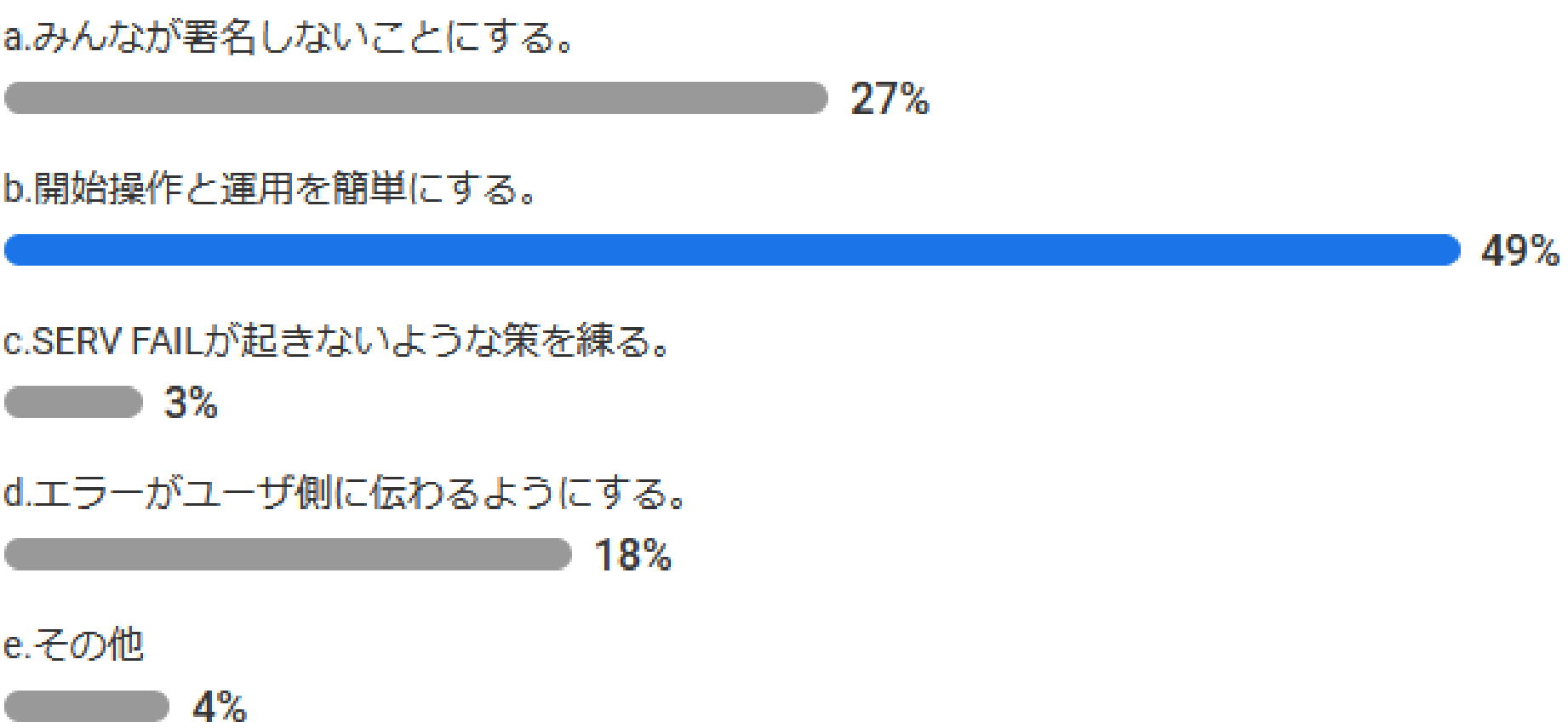

Sli.do #1142811

# 2. 技術導入にある”敷居”にどう向き合うか - DNSSEC署名 -

a. みんなが署名しないことにする。
   → (例) I-Dを書く。
b. 開始操作と運用を簡単にする。
   → (例) プロにおまかせする。
c. SERV FAILが起きないような策を練る。
   → (例)監視と運用
d. エラーがユーザ側に伝わるようにする。
   → (例)RFC化と実装
e. その他
   → [ご記入ください]

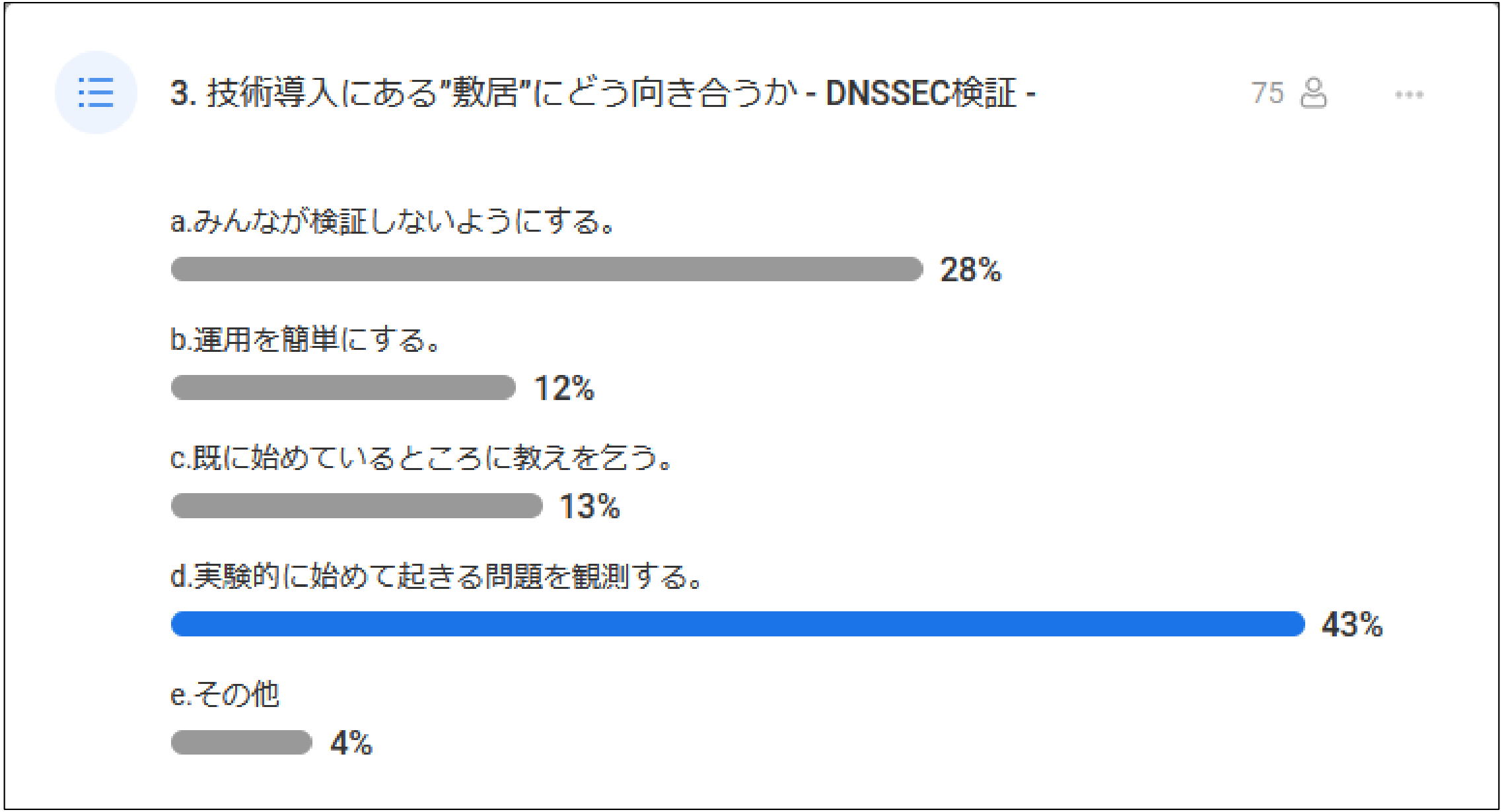
## 2. 技術導入にある"敷居"にどう向き合うか - DNSSEC署名 -

74



# 3. 技術導入にある”敷居”にどう向き合うか - DNSSEC検証 -

a. みんなが検証しないようにする。
   → パブリックキャッシュサーバは…
b. 運用を簡単にする。
   → (例) プロにおまかせする。
c. 既に始めているところに教えを乞う。
   → 問い合わせられたレコード中、署名されている割合は…
d. 実験的に始めて起きる問題を観測する。
   → どのような問題が…?
e. その他
   → [ご記入ください]


3. 技術導入にある"敷居"にどう向き合うか - DNSSEC検証 -
75
a.みんなが検証しないようにする。
28%
b.運用を簡単にする。
12%
c.既に始めているところに教えを乞う。
13%
d.実験的に始めて起きる問題を観測する。
43%
e.その他
4%

# おわり