IETF勉強会＆座談会より ～IETFオンラインとExtended DNS Errors～ ＋α

木村泰司, 塩沢啓

2021年6月4日(金) IETF勉強会＆座談会

主催：ISOC-JP、JPNIC　後援：WIDEプロジェクト　参加者**62名** 最大同時視聴数**59**

■ プログラム

15:00　開会

15:05　**リモート参加してみた&Tips**, 根津智子, 塩沢啓/JPNIC

15:30　IETFミーティング**参加に関わる座談会**
～時差が大きいとき他～　座談会

16:00　ライトニングトーク
- **IETF110頃からのMPLSの最近のお話**, 栃尾祐治氏 (ISOC-JP ispc,富士通)
- **Webのトランスポート関連(仮)**, 後藤ひろゆき氏

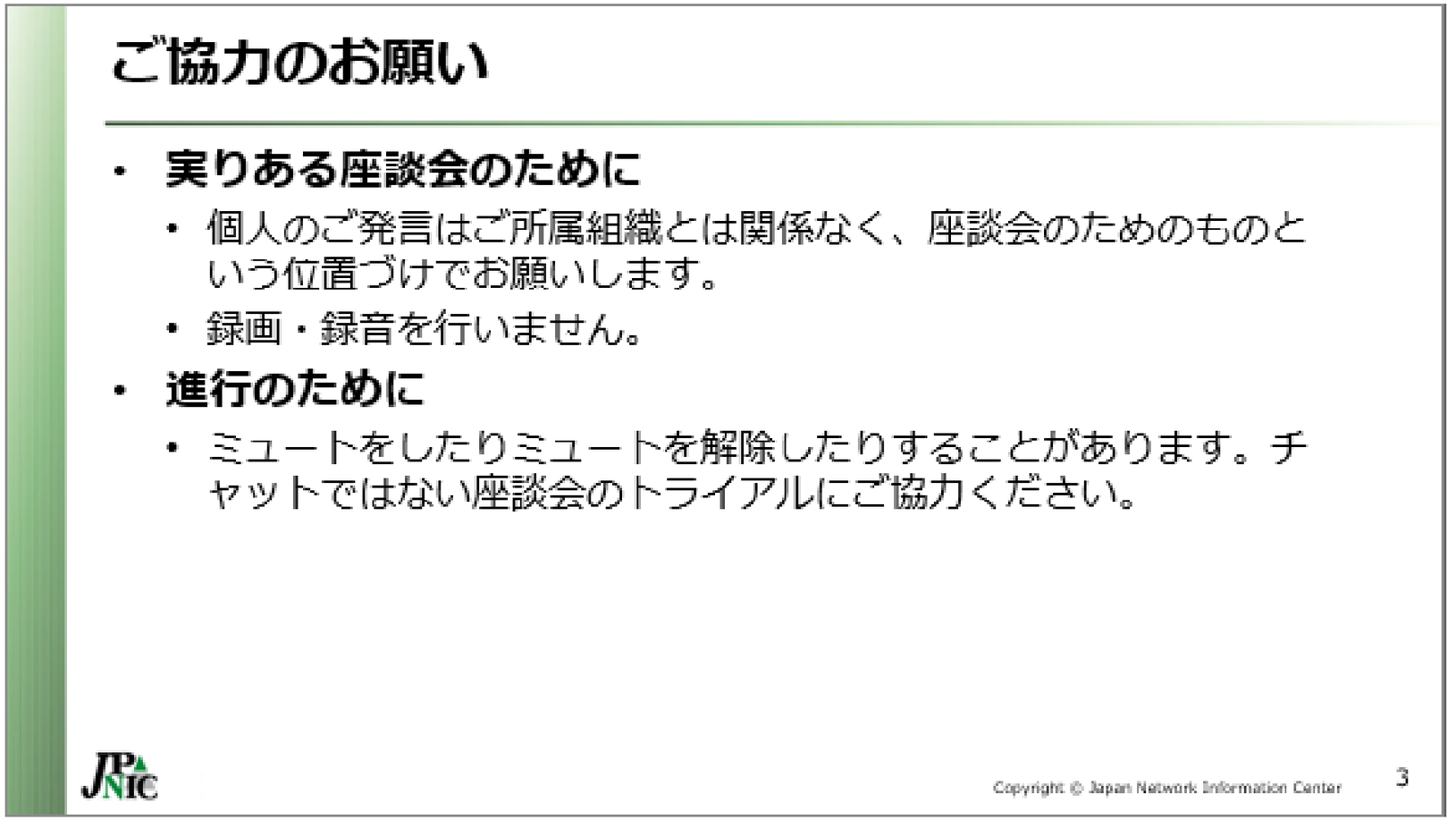
16:20　**旬の話題の座談会**
～**Extended DNS Errors (RFC8914)**～　座談会

17:00　閉会

発言のしやすさのため、ストリーミング配信・録画なし。

座談会のために…質疑応答は

- **Q&A機能、Slack、音声(手を挙げる必要なし)など、なんでもあり。**



IETFミーティング参加に関わる座談会 ～時差が大きいとき他～

- **時差について**
  - リモートワークだとダブルワーク
  - 深夜残業。社内の制度ののの兼ね合い。
- **仕事との兼ね合い**
  - 職場の理解
  - 朝の生活時間帯。一人で交渉しないとならない？
  - コアタイム。

ライトニングトーク

- IETF110頃からのMPLSの最近のお話, 栃尾祐治氏(ISOC-JP ispc,富士通)　https://bit.ly/3fEcnQA
  - 新しいMPLSラベルスタックに関するI-Dの紹介。関連するインターネットドラフトが急増中。デザインチーム（Open MPLS DT）が立ち上がっている。今後、MPLSラベルスタックの定義が後方互換性を維持しつつ更新され、新たなネットワーキングやアプリケーションが生まれるかもしれないとのこと。
- Webのトランスポート関連(仮), 後藤ひろゆき氏
  - QUICのRFCが公開。最近設立 WebTransport WGで主要I-D決定。
    - RFC8991 Version-Independent Properties of QUIC
    - RFC9000 QUIC: A UDP-Based Multiplexed and Secure Transport
    - RFC9001 Using TLS to Secure QUIC
    - RFC9002 QUIC Loss Detection and Congestion Control

旬の話題の座談会
～Extended DNS Errors (RFC8914)～

Extended DNS Errors (RFC8914)とは (1/2)

- **DNSの応答における状態を示すコード**：NOERROR(エラーなし)・NXDOMAIN(名前が存在しない)・REFUSED(拒否された)・SERVFAIL(サーバ側の異常)等があった。
- これらを**拡張するとより詳しいエラーの内容、例えばDNSSECのエラーの内容を返すことができる。そのためSERVFAILだけでは失敗の理由が分からなかったものがより分かり易くなる。**

■時系列・議論されている所

2017年2月
- Warren Kumari氏(Google)ら4名のIndividual Draft投稿。当初は lame や TooBusy も。

2017年10月
- dnsop WGのDraftとして投稿。

2018年6月
- 再投稿。現在の形に近い形に。

2019年7月
- エラー内容が整理される(-07)。

2020年10月
- RFC8914

■拡張されたDNSエラーコード (RCODE)
- サポートされていないDNSKEYアルゴリズム
- サポートされていないDSダイジェストタイプ
- 古くて無効な応答内容
- **改ざんされた応答内容**
- **DNSSECの検証結果は「偽」**
- DNSSECの検証結果は「不確定」
- **署名の期限切れ/まだ有効でない**
- 署名鍵が見つからない
- 署名のレコードが見つからない
- NSECが見つからない
- フィルタリングされた
- **ネットワークエラー**

など

■Extended DNS Errorsを使うにあたって考えるべきこと
- 拡張を含めるためにはEDNS0を扱うことができる必要
- エラーそのものを認証することはできない
- 受け取ったクライアントはどうすれば？

三つの立場

Extended DNS Errors (RFC8914)とは (2/2)

安心して
使いたい立場

エンドユーザ

- 「つながらない」
  その時どうする？(どう案内されてると良い？)

- アプリケーションはどうするか。
  - DoHをDNS,DNSSEC(DMARC)の検証のために使うのがいいのではないか。DANE、SPFの検証も。
  - ユースケース、Webアプリケーションで使えるようにする。

DNSSEC検証する
キャッシュサーバ

ネットワーク
サービス提供の立場

- そもそも検証開始をどう判断する？

- DoHサーバ
  - アプリケーションに署名状況やエラーが分かるようにする。draft-addy-dnsop-error-page

権威サーバ

オンラインの
サービス提供の立場

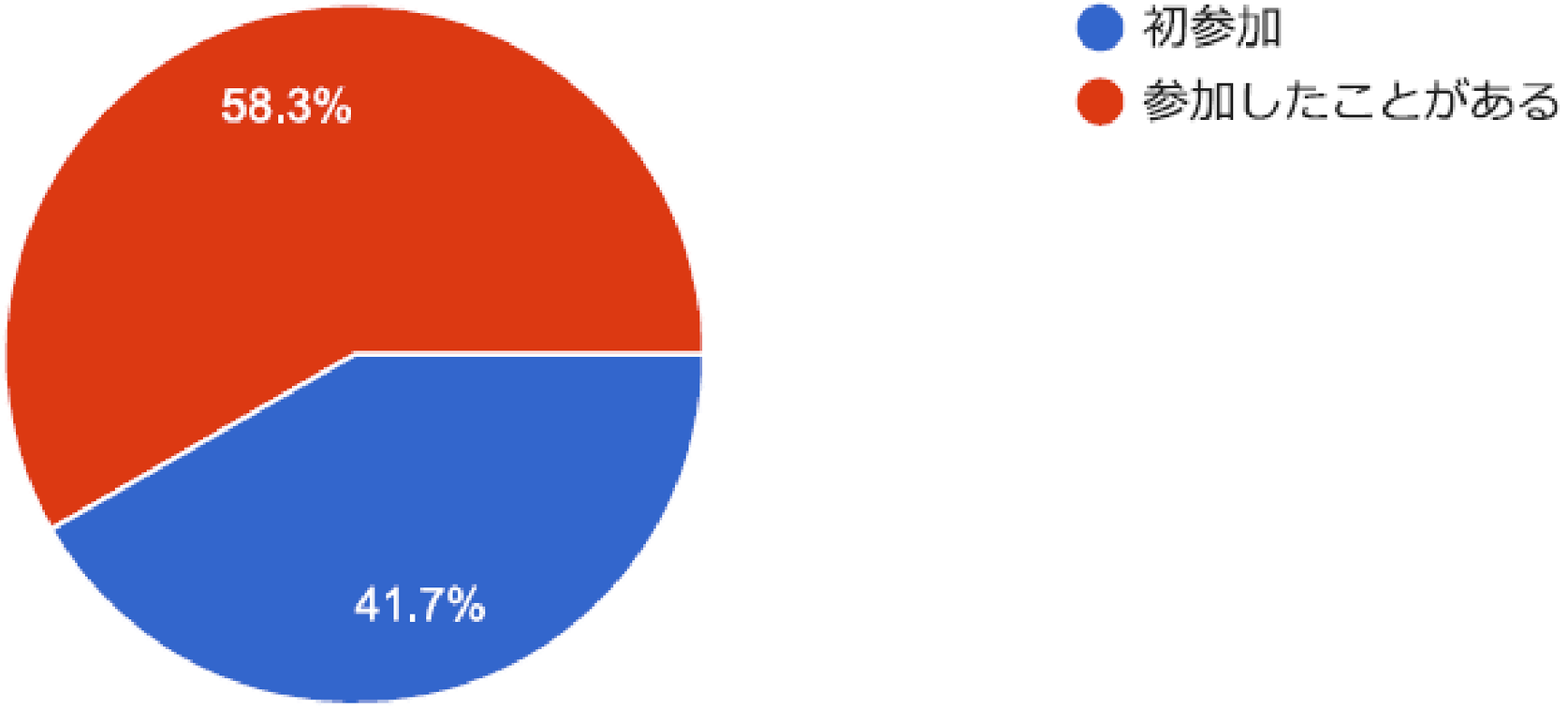
- そもそも署名開始をどう判断する？
- エラーが伝えられるなら変化も？

- 積極的に提供しずらい。
- メリットが理論的には分かるがサービス提供上よりも、何かあったらいやだなという気持ち

アンケートの結果

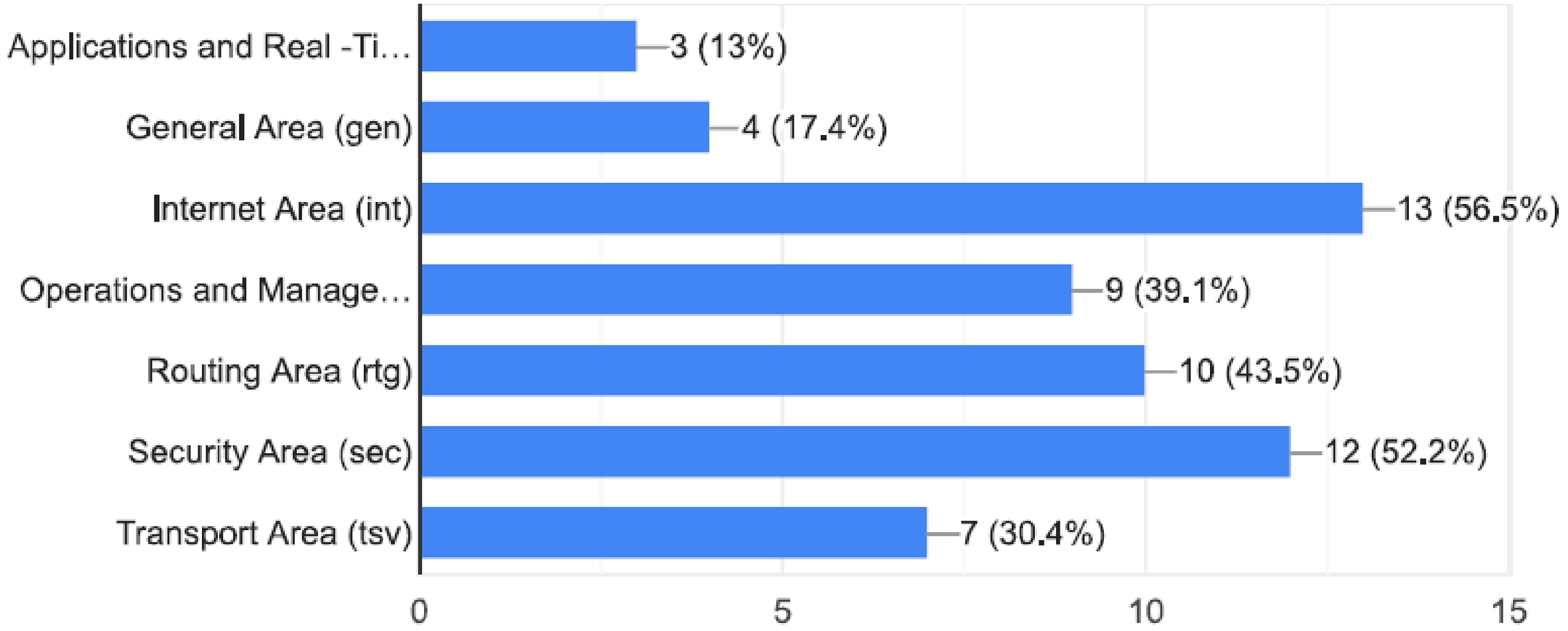
Q1. ISOC-JP/JPNIC主催の「IETF勉強会&座談会」や「IETF報告会」に、今まで参加したことがあるか、教えてください。

24 件の回答



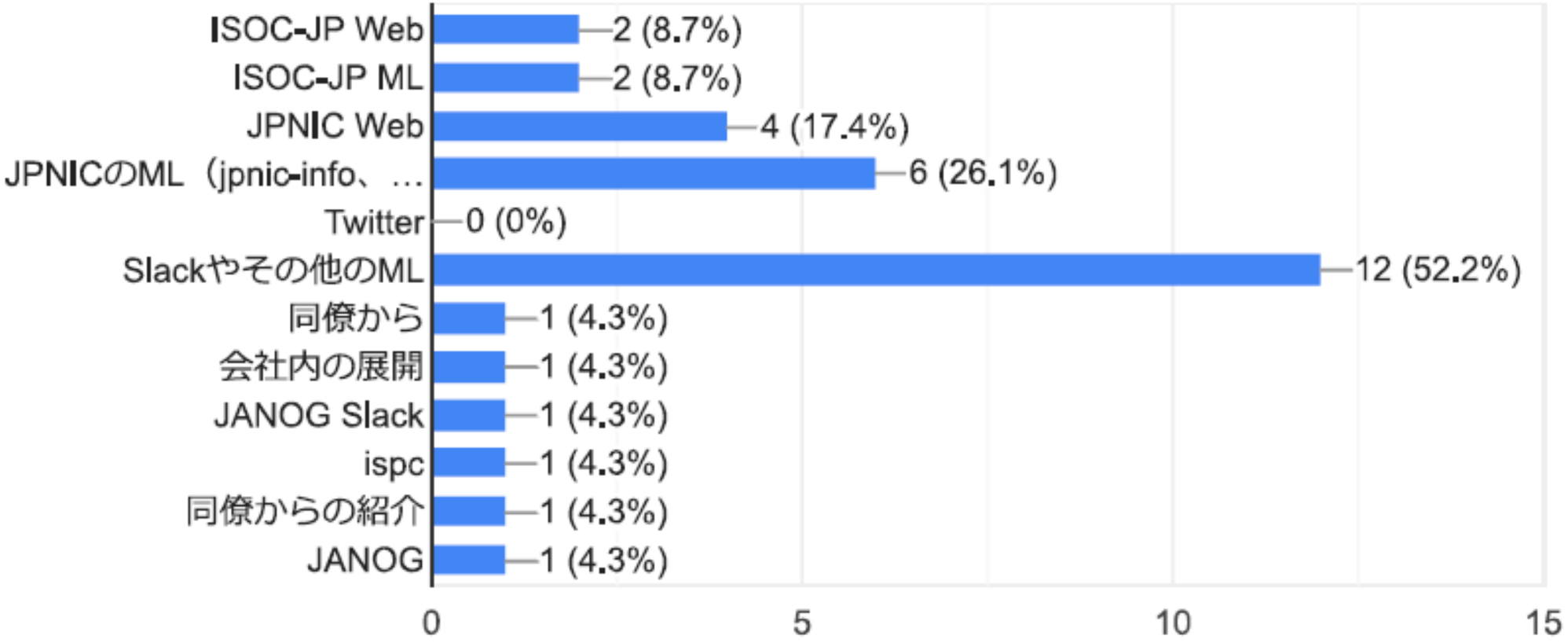
Q2. 関心をお持ちのIETFエリアをチェックしてください。特に関心の高い活動(WG/BoF/ML)があればその他にご記入ください。

23 件の回答



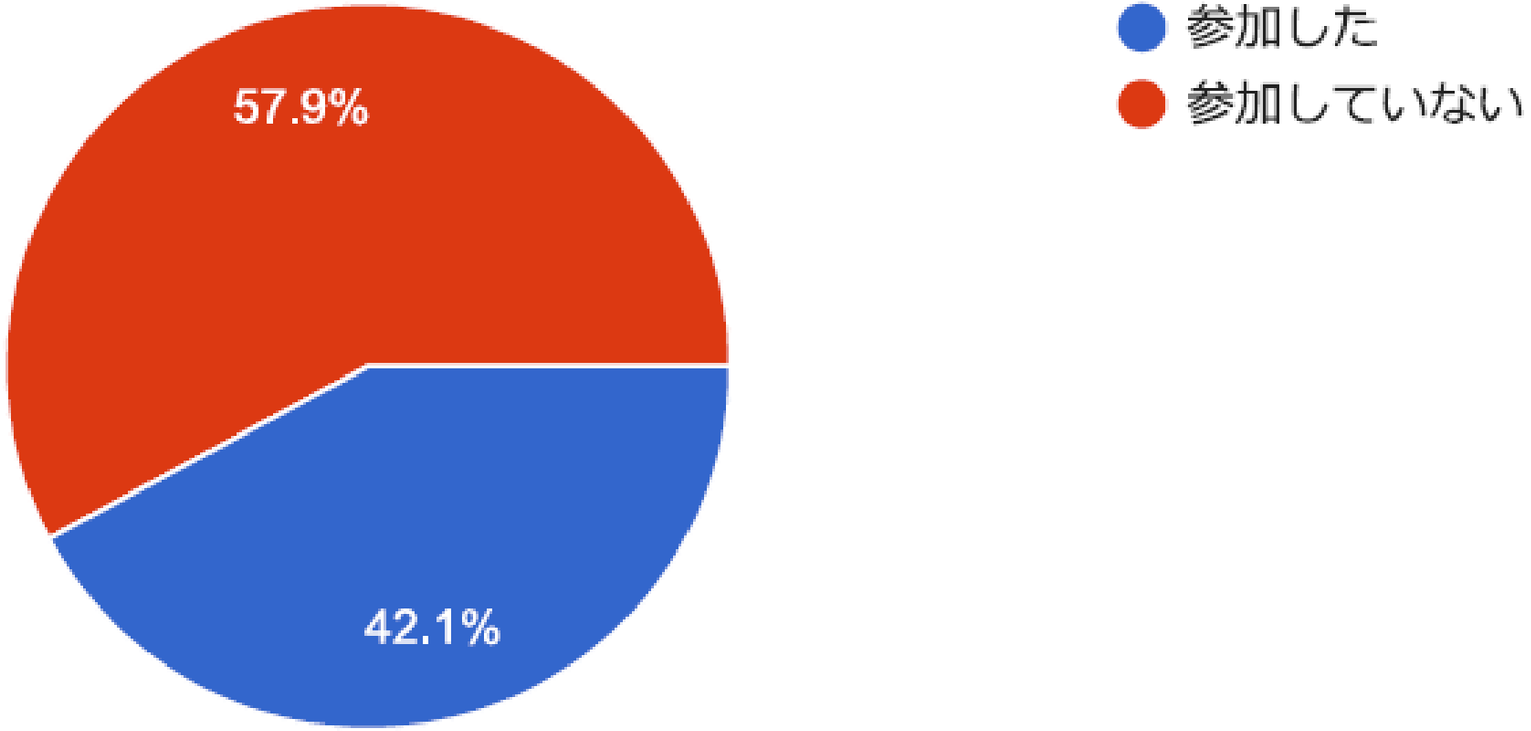
Q3-1. 今回の勉強会＆座談会はどの媒体でお知りになりましたか？「その他のSlackやML」と回答された方は団体名 (ietf-jp / JANOG / TDNOG / ENOG / QUNOG / WIDE / セキュリティキャンプ他)を、その他にご記入ください。

23 件の回答



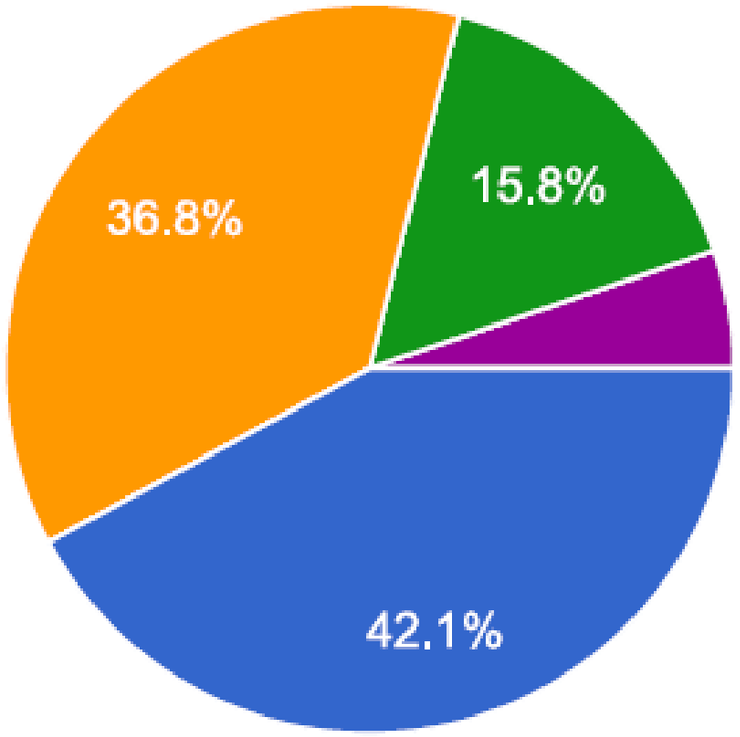
Q4-1. これまでIETFのML、BoF、WG Meetingに参加した事がある方にお伺いします。IETF 110th Onlineには参加されましたか。

19 件の回答



Q4-2. 今後もIETFへの参加を継続する予定ですか。

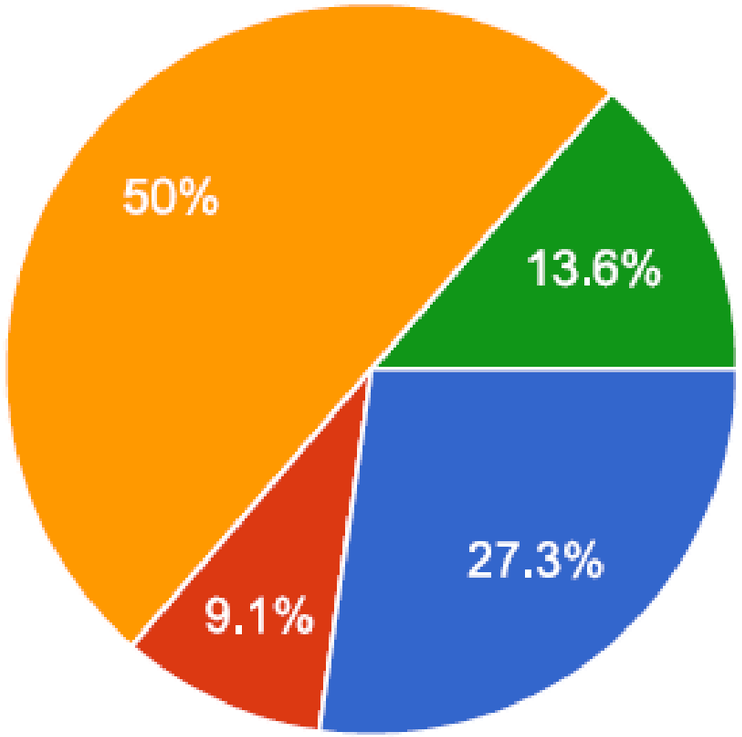
19 件の回答



- 現地開催/オンライン開催に関わらず参加予定
- 現地開催なら参加予定
- オンライン開催なら参加予定
- いいえ
- 未定

Q5. 今後IETFに参加してみようと思いましたか。

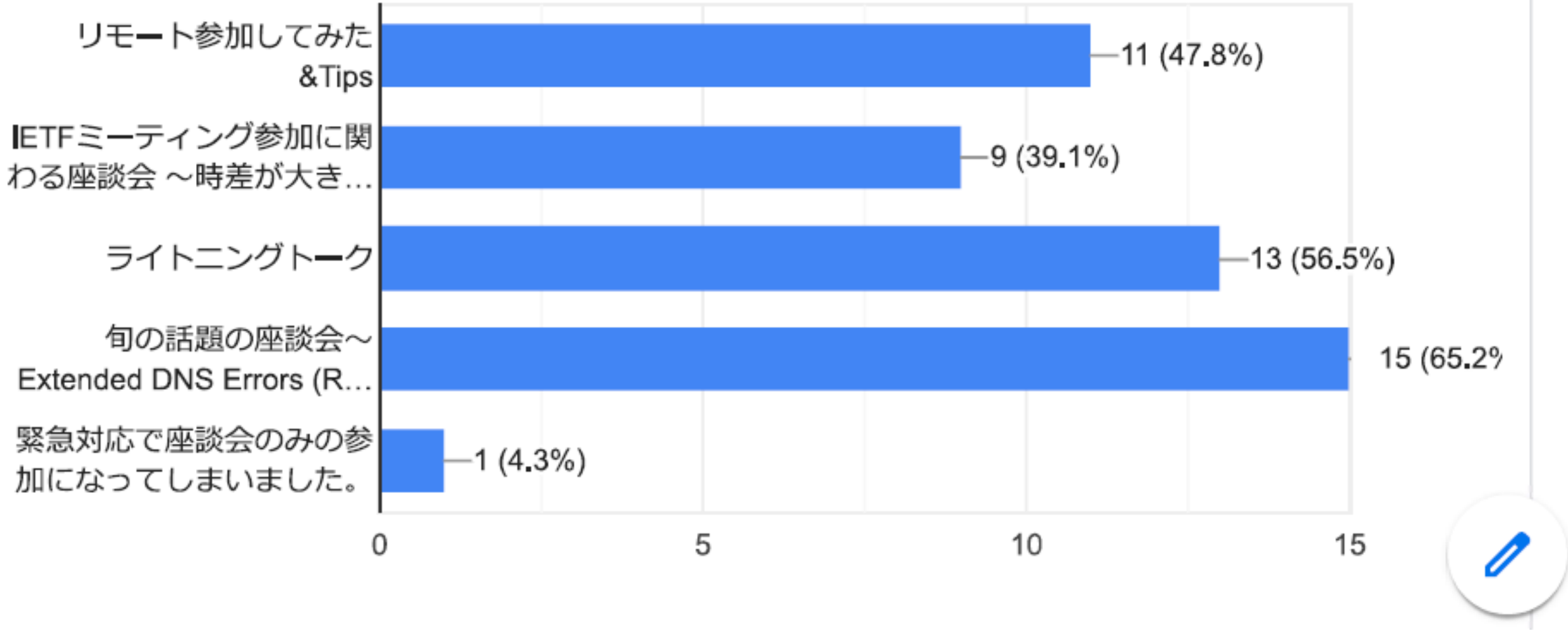
22 件の回答



- もともと参加する予定だった
- これを機に参加してみようと思う
- 今後のIETFの動向を踏まえて判断する
- 参加しないが、このようなイベントには参加したい
- (報告会も含め)自分には関係なさそうに思った

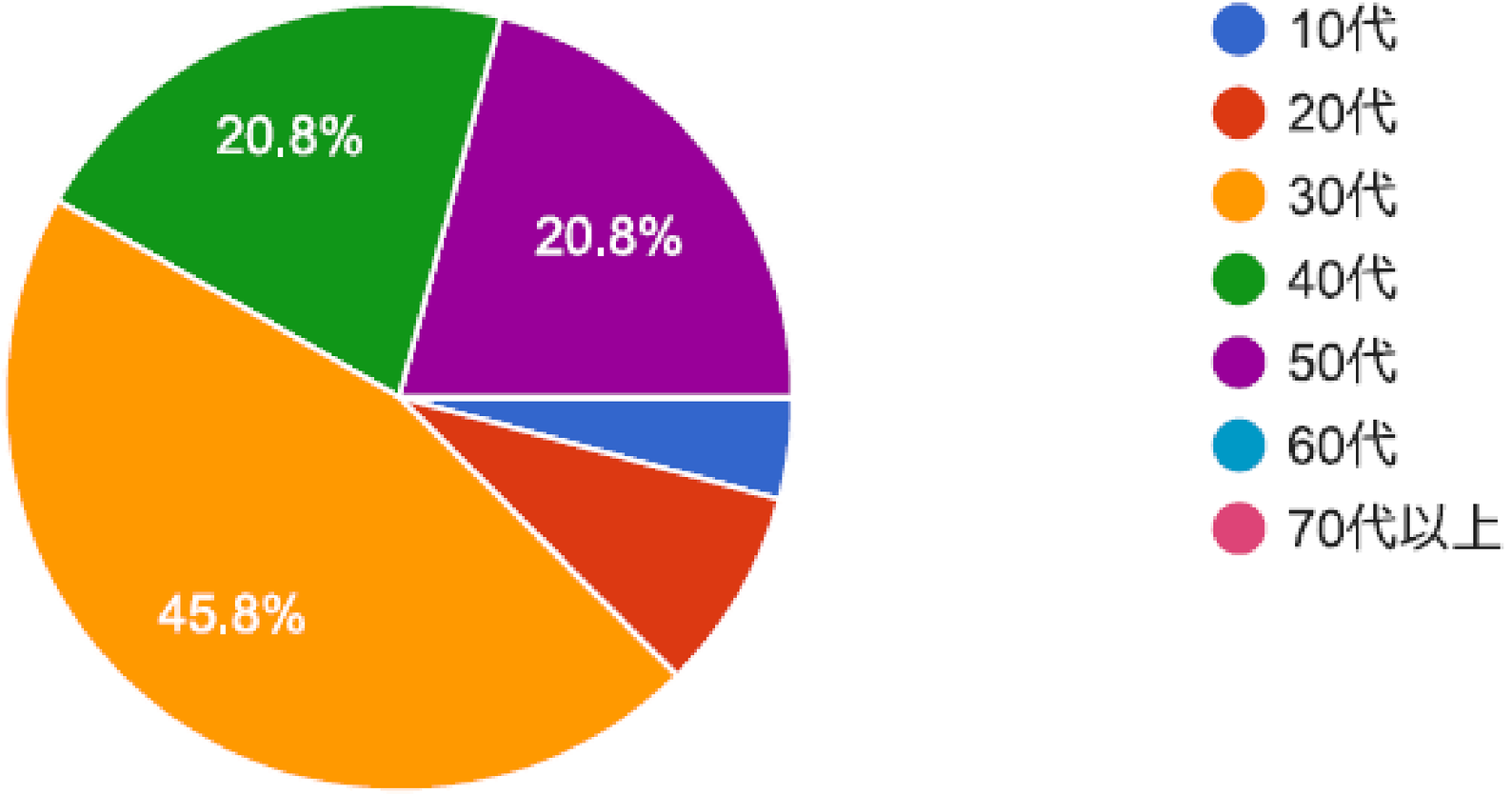
Q6. 本日のプログラムの中で、満足度が高かったセッションを教えてください(複数回答可)。

23 件の回答



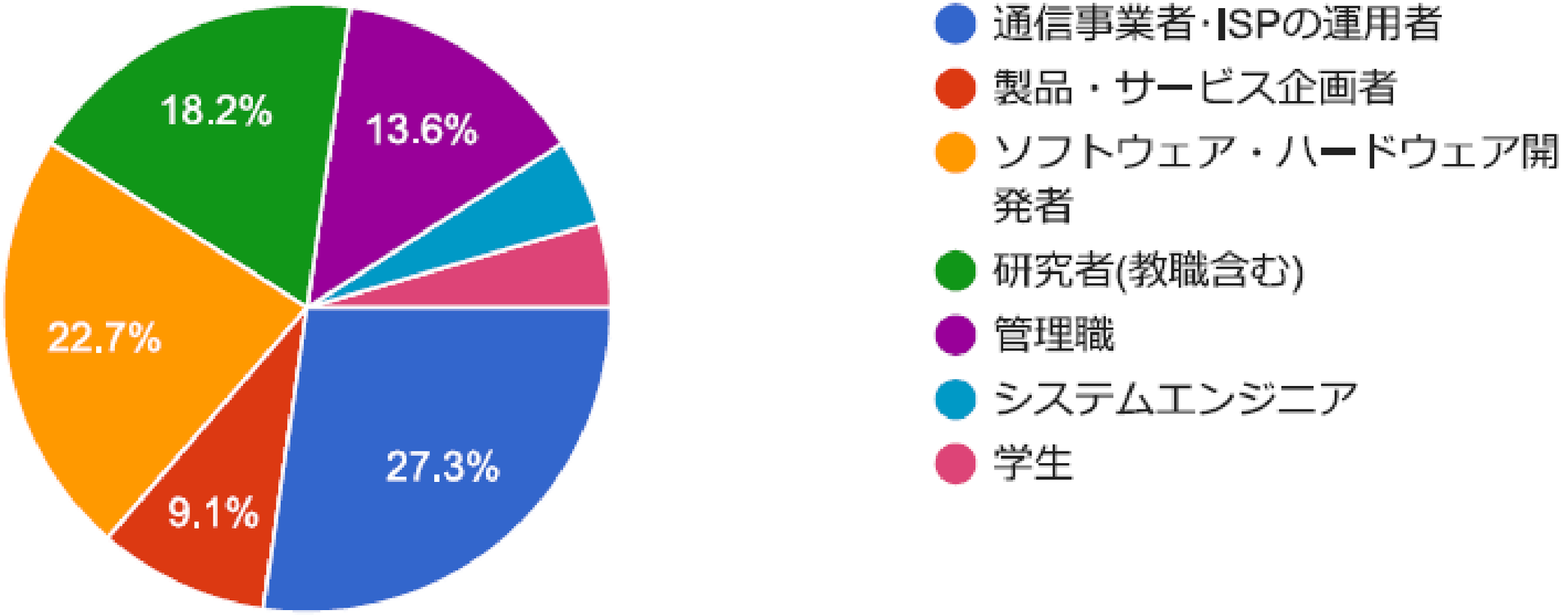
Q7. あなたの年齢を教えてください。

24 件の回答



Q8. あなたの職種を教えてください。以下に適切なものが無ければ差し支えない範囲で教えてください。

22 件の回答



まとめとご質問

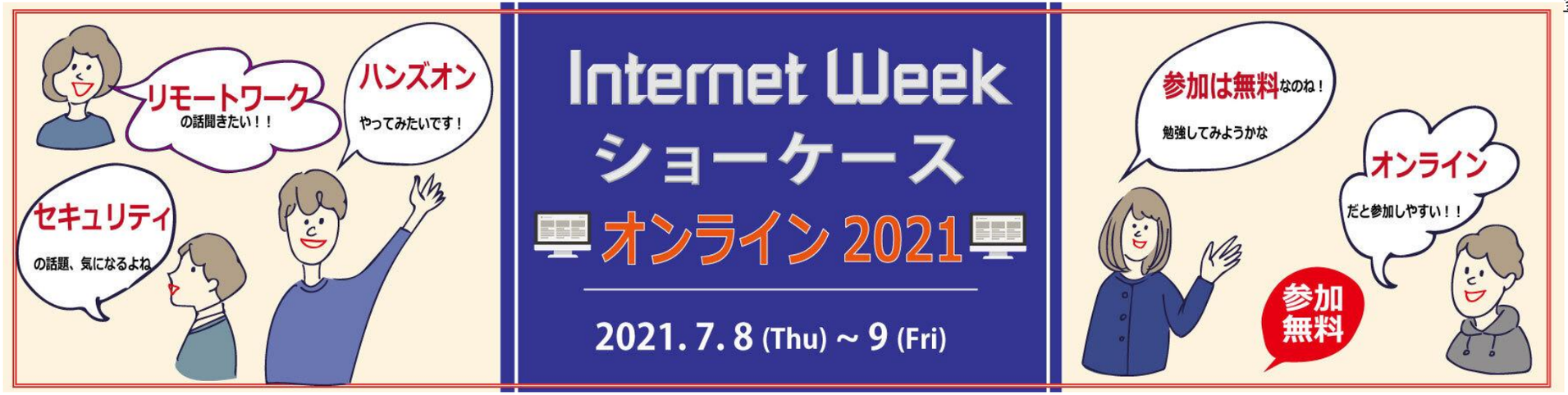
- **「座談会」としたことで**
  - 情報交換や意見交換は比較的活発だった模様！ネタ次第？
- **リモート参加であるために**
  - 敷居の低さも
    - 議事メモは充実
    - 動画閲覧
  - 厳しさ
    - 時差 → 24時間働けますか状態(いいすぎ
  - 現地ならでは
    - 立ち話はやはり重要

「座談」に向いているネタはありますか？

- Web
- ネットワーク
- 標準化 3GPP...
- 災害
  :

+α とは…「お知らせ」

Internet Week ショーケース オンライン 2021



参加登録はこちらから！

- 日程：2021年7月8日(木)～7月9日(金) *https://www.nic.ad.jp/sc-2021/*
- 参加費：無料
- 開催形態：オンライン
- 現在、参加申込受付中！

プログラム 1 ーオンラインでもセキュリティログ分析を体験

・7月8日(木) ハンズオンプログラム

参加登録はこちらから！

10:00
～
16:00

Elasticsearch+Kibanaによるセキュリティログ分析ハンズオン

講演者


中島 章博

中島 章博(アマゾン ウェブ サービス ジャパン株式会社)

概要

脅威ハンティング、検知済みの脅威への対応、 フォレンジックなどのセキュリティ対応においてログ分析は重要な作業です。 これを助けるツールとしてSIEMと呼ばれる製品群が挙げられますが、 導入していても有効に活用できていない、 高価なため導入に踏み切れないケースがしばしば見られます。 本ハンズオンではオープンソースのRESTfull分散検索/分析エンジンであるElasticsearchを中心にセキュリティログ分析基盤を活用し、 セキュリティインシデントの分析・調査を体験します。

本ハンズオンでは、 講師が用意した環境をハンズオン環境として利用しながら、 セキュリティログ分析に特化した内容を中心に説明、体験します。 Elasticsearchそのものの導入(インストール)はハンズオンの対象外ですが、 参加者はGitHubで公開されているOpen Distro for Elasticsearchを利用することで同一の環境をオンプレミスを含むさまざまな環境で構築することが可能です。

プログラム

第一部 セキュリティログ分析 体験

あらかじめ用意されたシナリオに則ってセキュリティログ分析を体験します。 一環としてクラウドが出力するセキュリティ上重要なログや、 それらを出力するサービスについても解説します。

第二部 セキュリティログ分析基盤の設計と構築

第一部ではあらかじめ用意されていたログ分析環境を利用しました。 実際にこのような基盤を構築するにあたって検討するべき勘所を解説し、 実際に構築を行います。

プログラム２ －「リモートワーク」や「法制度」の新プログラムも

・7月9日(金)　カンファレンスプログラム

参加登録はこちらから！

- **リモートワークを支える社内セキュリティ基盤の作り:**
  - 水谷 正慶氏(クックパッド)
- **これからのメールセキュリティ**
  - 平野 善隆氏 (JPAAWG/クオリティア)
  - 櫻庭 秀次氏 (JPAAWG/インターネットイニシアティブ)
- **脅威インテリジェンスの活用方法**
  - 石川 朝久氏 (東京海上ホールディングス)
- **プロ責法・個人情報保護法の近時の法改正とその影響**
  - 上沼 紫野氏 (虎ノ門南法律事務所)
  - → IWショーケース特別企画のプログラム！

JPNICなどなど