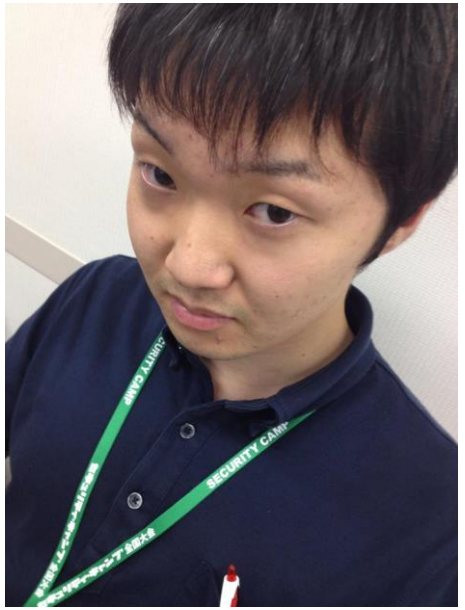
CTF for Beginners

～今日までそして明日から～

話者プロフィール

- 保要 隆明 (@takahoyo)
  - 講習ではネットワーク解析を担当。ムードメーカー。
  - 普段はネットワークセキュリティの研究をしてます。
- 三村　聡志 (@mimura1133)
  - 講習ではバイナリ解析を担当。代表。
  - 普段は Windows なソフト開発と解析をしてます。



CTF for Beginners を始めるまで

- 最初は
  “CTF for Girls” の “Boys 版” の話から

- “CTF for Boys” ではなく
  誰でも参加できる勉強会ということで
  “CTF for Beginners” に

CTF for Beginners を始めるまで

- 開始するまでに必要なこと
  - 運営メンバー集め
  - 講習形式をどうするか
  - 会場をどうするか
  - どうやって受講者を集めるか
  - 講習内容の構成の検討
    - 教材作り

CTF for Beginners を始めるまで

講義の内容

- ソフトウェア開発時や障害発生時の原因調査などでも幅広く活かすことができる内容
  - 実行ファイルの解析 → デバッグ
  - 通信の解析 → ネットワーク構築, 障害対応
  - Web アプリの脆弱性とその原因
    → 開発時に気づけるようにする
- 特にCTF だけに絞った内容にはなっていない

講義の内容

講義の内容

- CTFの説明
- バイナリファイル解析
- ネットワーク通信解析
- ウェブアプリの脆弱性
- 簡易CTF

CTF の説明

- CTF とはどのようなものか
  出題形式にはどのような物があるかを説明

- 許可されたサーバ　と
  自身で管理するサーバ
  以外に攻撃しないように釘を刺す
  - 不正アクセス禁止法や法律の考え方などの説明

- File コマンドによる種類の判定
  - 拡張子なしのファイルを判定して開く
- String コマンドによる文字列の抽出
- IDA Pro を使用した実行ファイルの解析
  - 実行先を変更するだけで答えが出るもの
  - コードを読んで難読化された文字を読む

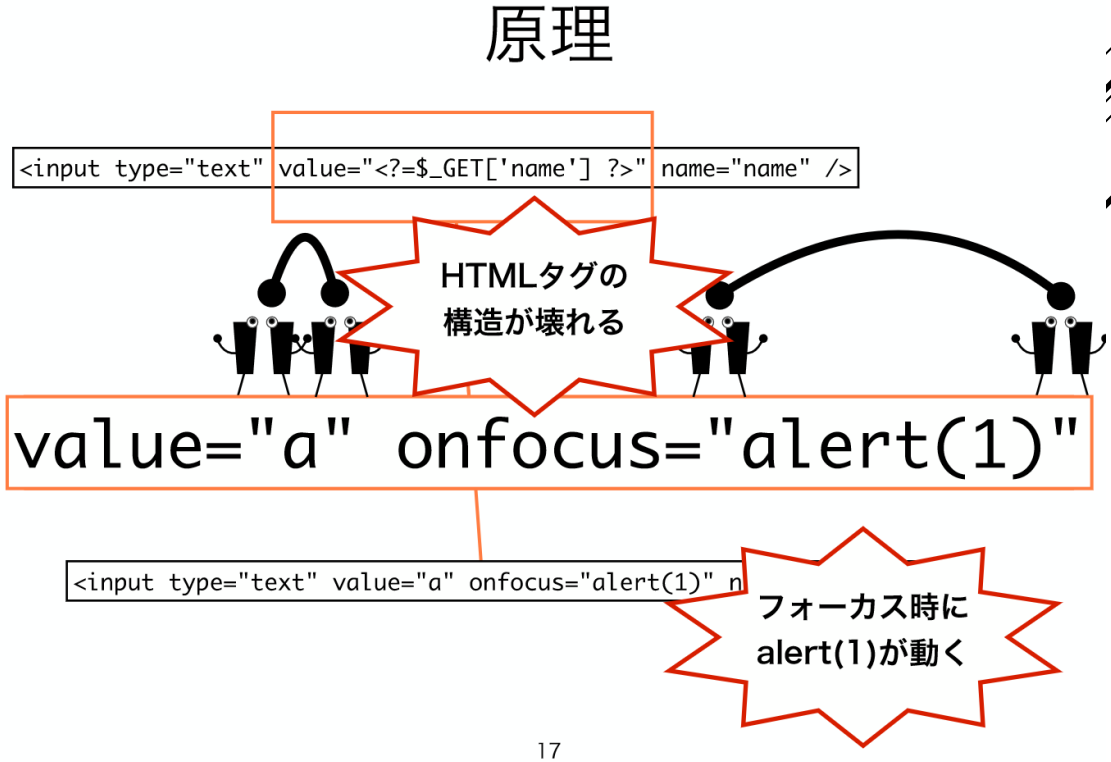
バイナリファイル解析

- ネットワーク解析の方法
  - キャプチャファイルとは何か
  - Wiresharkの使い方
  - Network Minerの使い方
  - その他、ネットワークツールの紹介
- ネットワークパケットを見るポイント
  - そのために何が必要なのかなど

ネットワーク通信解析

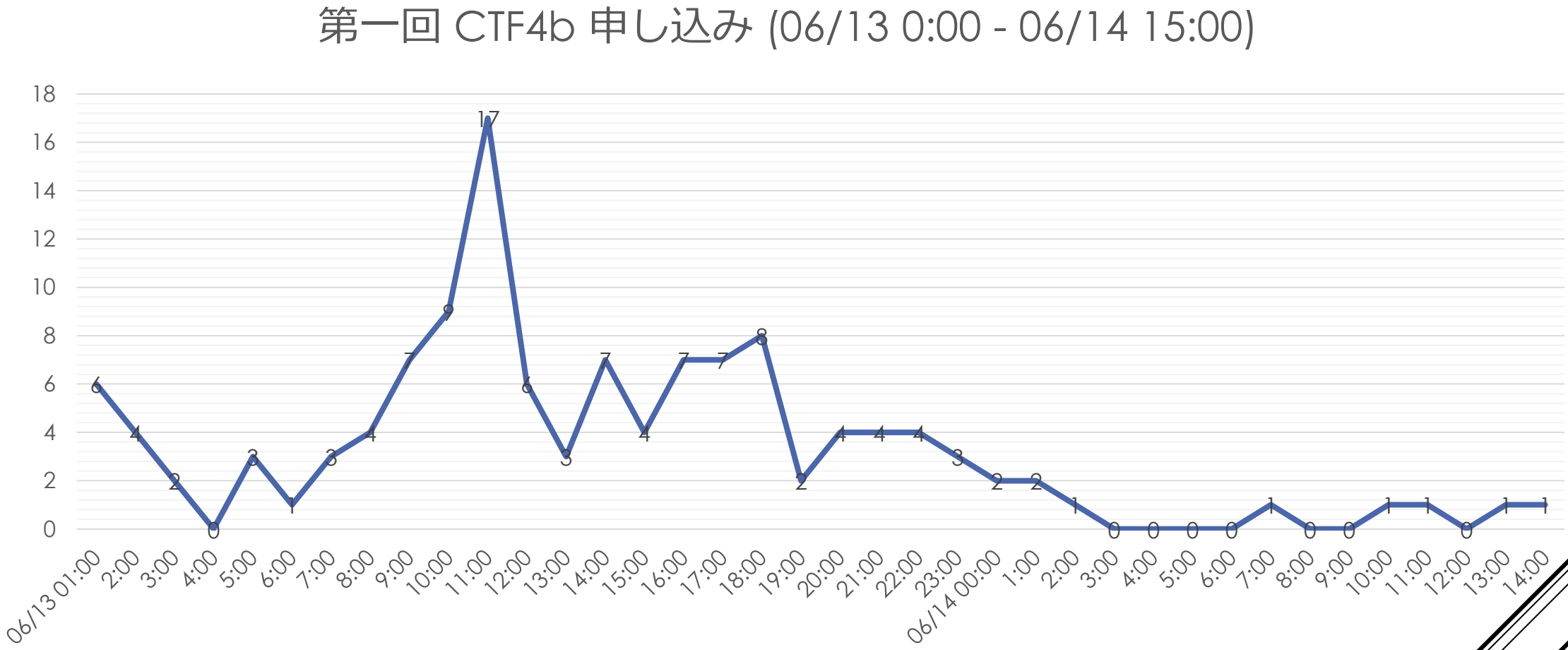
- XSS や CSRF，SQL Injection を取り扱う
  - 脆弱性はなぜ作り込まれるのかを
    その原因から説明する
- 攻撃方法とその対策方法を
  一緒に説明
- 開発時に「気づける」ように

ウェブアプリの脆弱性



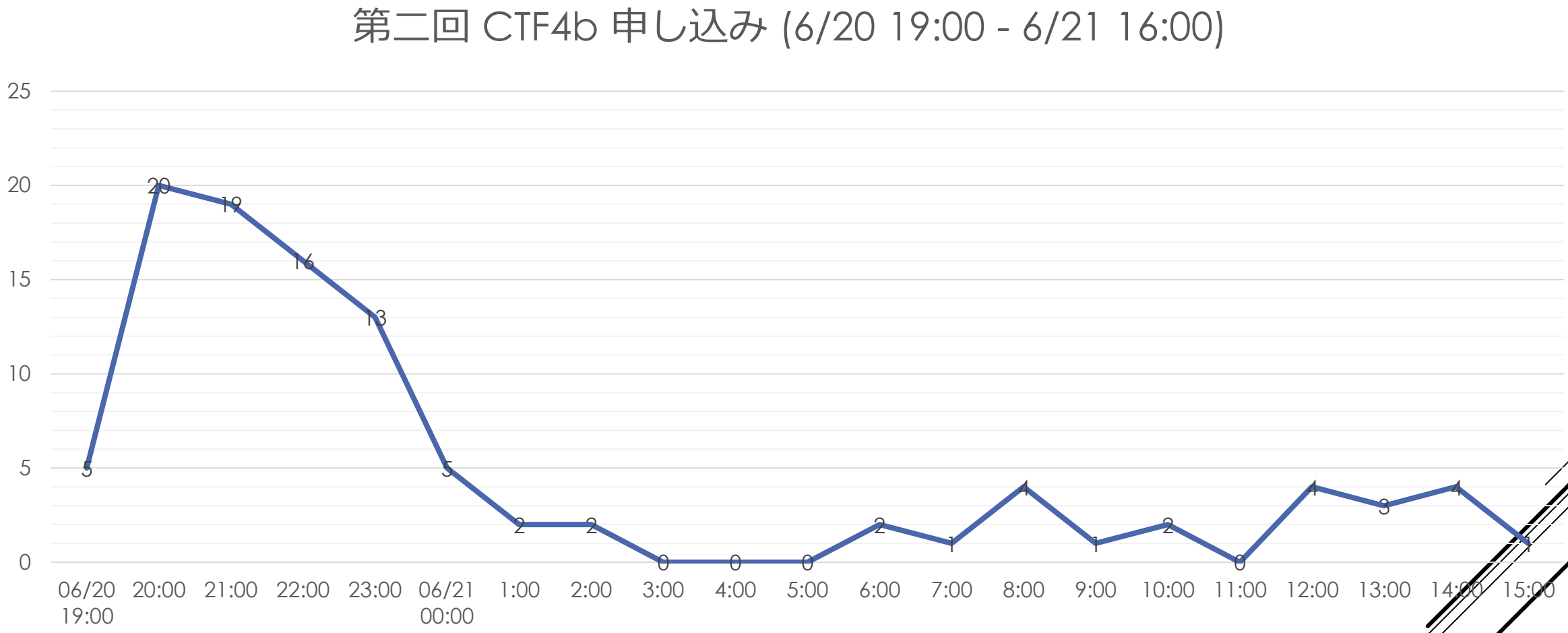
申し込み速度から見える注目度

アンケートから見えること



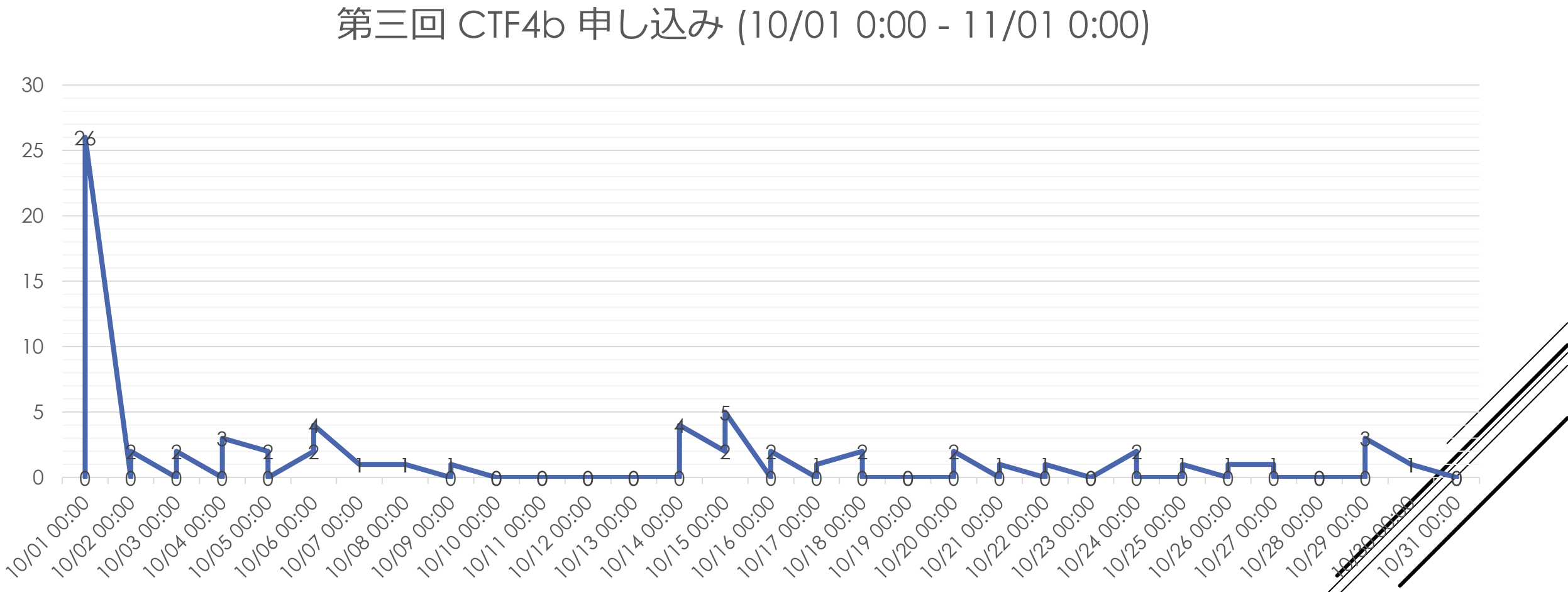
申し込み速度から見える注目度 (東京１)

3.8人 (毎時)



申し込み速度から見える注目度 (東京２)

4.95人 (毎時)



申し込み速度から見える注目度（福岡）

0.102人 (毎時)

申し込み速度から見える注目度

- 関東エリアでの注目度は高い
  - 東京（１回目）：125名
  - 東京（２回目）：104名
  - 福岡（３回目）：76名
- 東京エリアでは２回とも
  会場の定員に達したため募集を中断した
- 福岡開催にも関東からの参加者が存在した

事前アンケートから見える「情報セキュリティ」に対するイメージ

アンケートから見えること

- 集計方法
  - 申込時に
    「情報セキュリティと聞いて
    どのようなイメージを思い浮かべますか（自由記述）」
    という自由記述欄を設置
  - 回答を mecab (ipadic) により形態素解析した後、
    「名詞」と「形容詞」の出現頻度を算出
    意味をなす単語のうち上位５つを抽出した

「情報セキュリティ」に対するイメージ

- 名詞
  - 脆弱性（脆弱性の発見, 脆弱性を突く etc..）
  - 情報　（情報を守る, 情報漏洩, 情報の管理 etc..）
  - 攻撃　（攻撃への対抗, 攻撃を防ぐ etc..）
  - 知識　（知識のハードルが高い, 深い知識 etc..）
  - 人　　（人的リスク, 個人情報, 怖い人たち etc..）

「情報セキュリティ」に対するイメージ

- 形容詞
  - 難しい　（理解が難しい, 曖昧で小難しい, 難しいもの etc..）
  - ない　（わからない, 知らない, 守れない, 漏れない etc..）
  - こわい　（怖い人たち, 怖い etc..）
  - 広い　（分野が広い, 広い範囲の知識 etc..）
  - 深い　（深い知識, 広く深い知識が要求される etc..）

「情報セキュリティ」に対するイメージ

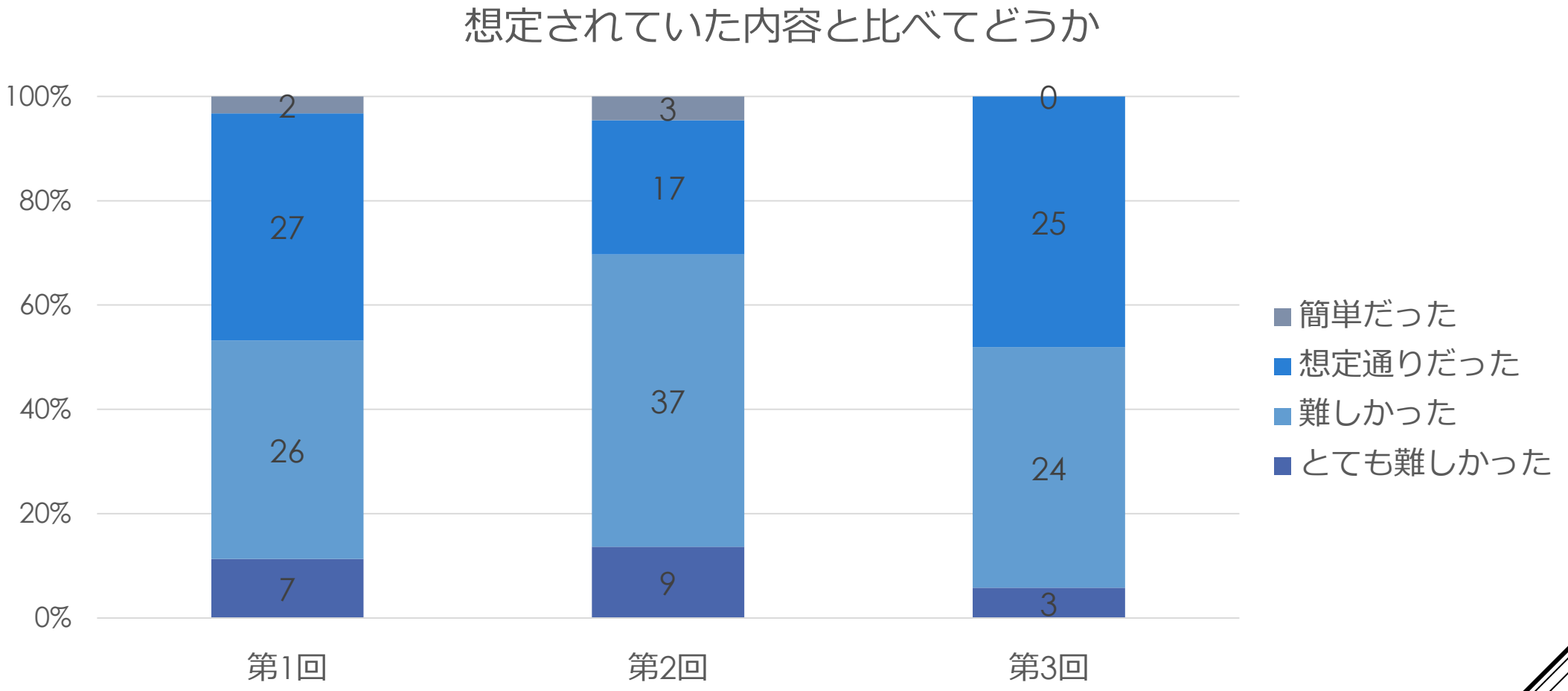
- 「怖いもの」としてのイメージが強い

- 「情報セキュリティ」を扱うために必要な知識がとても幅広いという印象も持たれている。
  - 「体系立っていない」というコメントもあった

「情報セキュリティ」に対するイメージ

事後アンケートから見える想定との乖離

アンケートから見えること


想定されていた内容と比べてどうか
100%
80%
60%
40%
20%
0%
2
27
26
7
3
17
37
9
0
25
24
3
第1回
第2回
第3回
簡単だった
想定通りだった
難しかった
とても難しかった

参加者の想定との差

- 時間が短かった
- 環境が重かった
- 本当の初心者にとっては少し難しかった
- 会場のネットワークが混んでてつらかった
- 答え合わせがもっと欲しかった
- etc..

感想からみる想定との乖離

感想と満足度

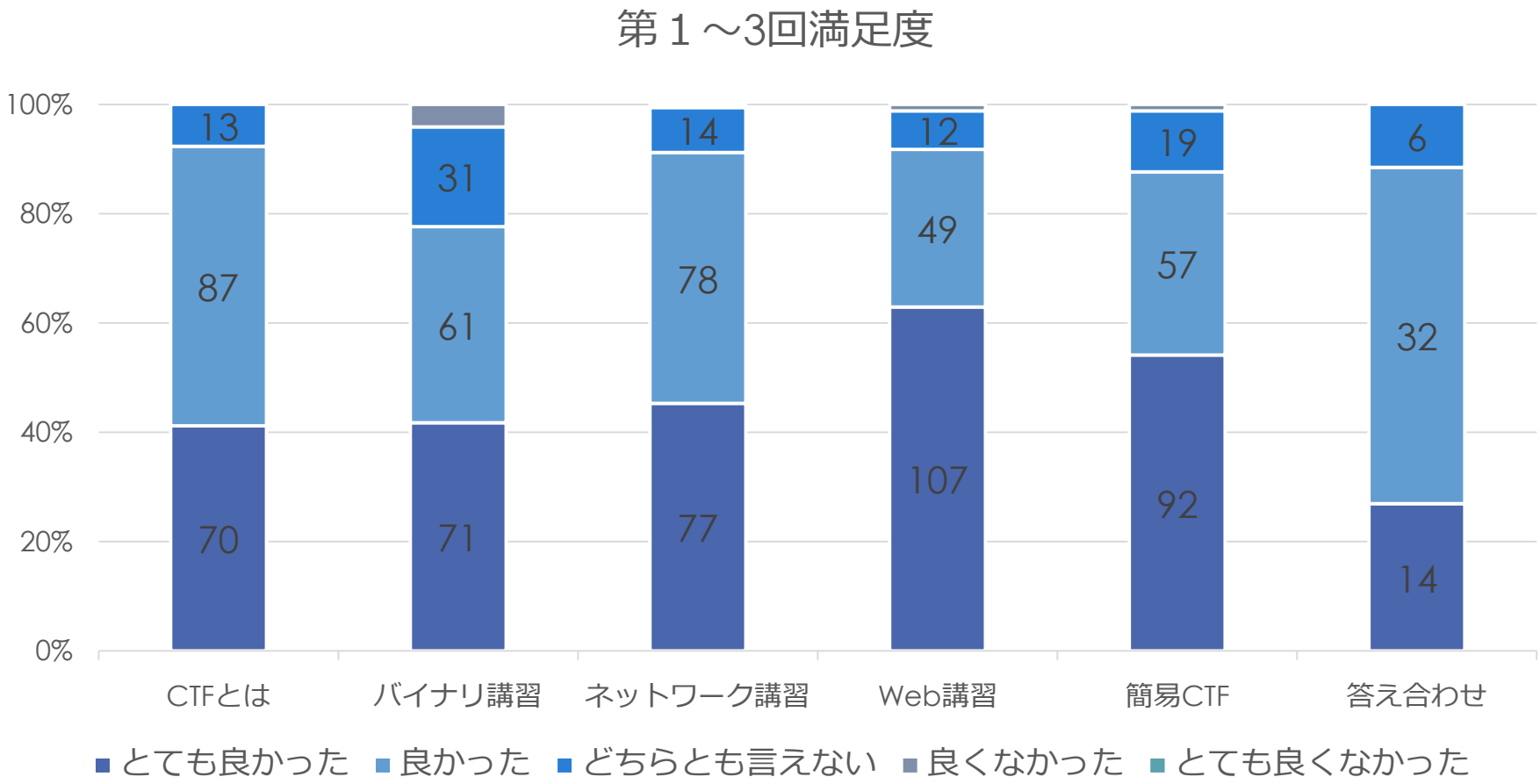
アンケートから見えること

- 意見・感想においては次のような単語が多かった*：
  - 良かった、良い
  - 楽しかった、楽しい、楽しく
  - 面白かった、面白い
  - etc..

- ポジティブな感想が多い

感想

*事後アンケートにおいて回収した
意見及び感想を mecab (ipadic) により形態素解析し、
上位の「形容詞」を列挙したもの


第１～3回満足度
100%
80%
60%
40%
20%
0%
13
87
70
31
61
71
14
78
77
12
49
107
19
57
92
6
32
14
CTFとは
バイナリ講習
ネットワーク講習
Web講習
簡易CTF
答え合わせ
とても良かった
良かった
どちらとも言えない
良くなかった
とても良くなかった

セッションの満足度

- もっと長い時間にして欲しい
- もっと地方でも開催して欲しい
- 情報収集の仕方を含めて教えて欲しい
- 最初の一歩になるように今後も続けて欲しい
- Beginner向けの大会を開いて欲しい
- etc..

要望

今後の課題