

2018年度 デジタル・フォレンジック 普及状況調査結果

2019年3月
「DF普及状況調査」WG

目次

1. DF普及状況調査の目的	… 2
1.1. DF普及状況調査の手法と取得件数	… 3
2. アンケート集計結果	
2.1. ご自身の所属組織は？	… 4
2.2. ご自身の現在の立場を教えてください	… 5
2.3. デジタル・フォレンジックの活用経験は？	… 6
2.4. ご自身が「デジタル・フォレンジック」に関わる立場を教えてください	… 7
2.5. 現在関係している「デジタル・フォレンジック」の分野は？	… 8
2.6. 「デジタル・フォレンジック」の対象として思い浮かぶものは？	… 9
2.7. 最も有望なビジネス分野はどこですか？	…10
2.8. デジタル・フォレンジックの有益な活用分野はどこですか？	…11
2.9. デジタル・フォレンジック分野に影響を及ぼす国内外の法改正は？	…12
2.10. 使ったことのあるツールを教えてください	…13
2.11. 海外ツールを使用する際の課題や問題点は？	…15
2.12. デジタル・フォレンジックに期待する分野・方向性、今後の調査項目等について	…16
3. 考察と今後の取り組み	…18

1. DF普及状況調査の目的

デジタル・フォレンジックは、情報漏洩や不正アクセスなど問題発生時の解決手段として、また証拠能力がある情報を得る手段として活用され、ICT分野における必須の技術として発展してきた。

しかし残念ながら、デジタル・フォレンジックは、第三者に知られたくない場面で利用されることが多く、その普及状況はセキュリティ製品やサービスと比較しても、あまり知られていない。

そこで、デジタル・フォレンジック製品やサービスの導入・使用状況や、デジタル・フォレンジックを活用する関係者の認識や、ユーザの期待を調査することで、IDF活動への反映や会員および企業・団体会員のインセンティブとなるデータをまとめることを目的として取り組むこととする。

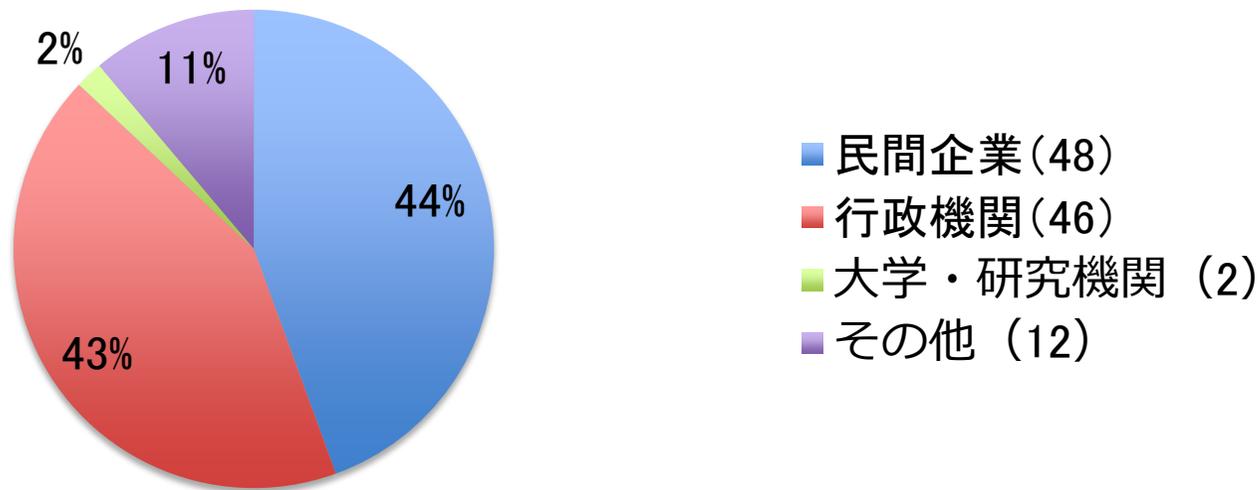
1.1. DF普及状況調査の手法と取得件数

デジタル・フォレンジックの普及状況等について、定性・定量的な経年変化を分析するため、毎年定点観測的にデータ収集を行っている。

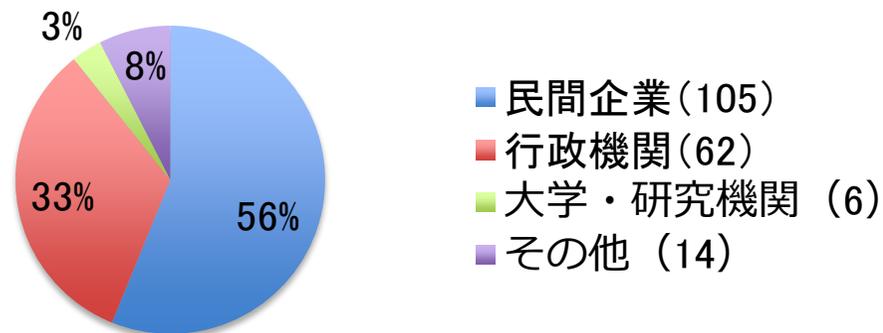
2018年度の調査では、コミュニティ2018のセミナープログラムに「30分間のWEBアンケート」を設けて実施し、WEBアンケートと紙アンケートを併用し108名の協力を得ることができた。

アンケートは「設問への投票」と「自由記入コメント」に加え、「自由記入コメント」に対する「賛同票」と「反対票」の投票を受け付け、アンケート回答者の生の意見を吸い上げる取り組みを行った。

2.1. ご自身の所属組織は？

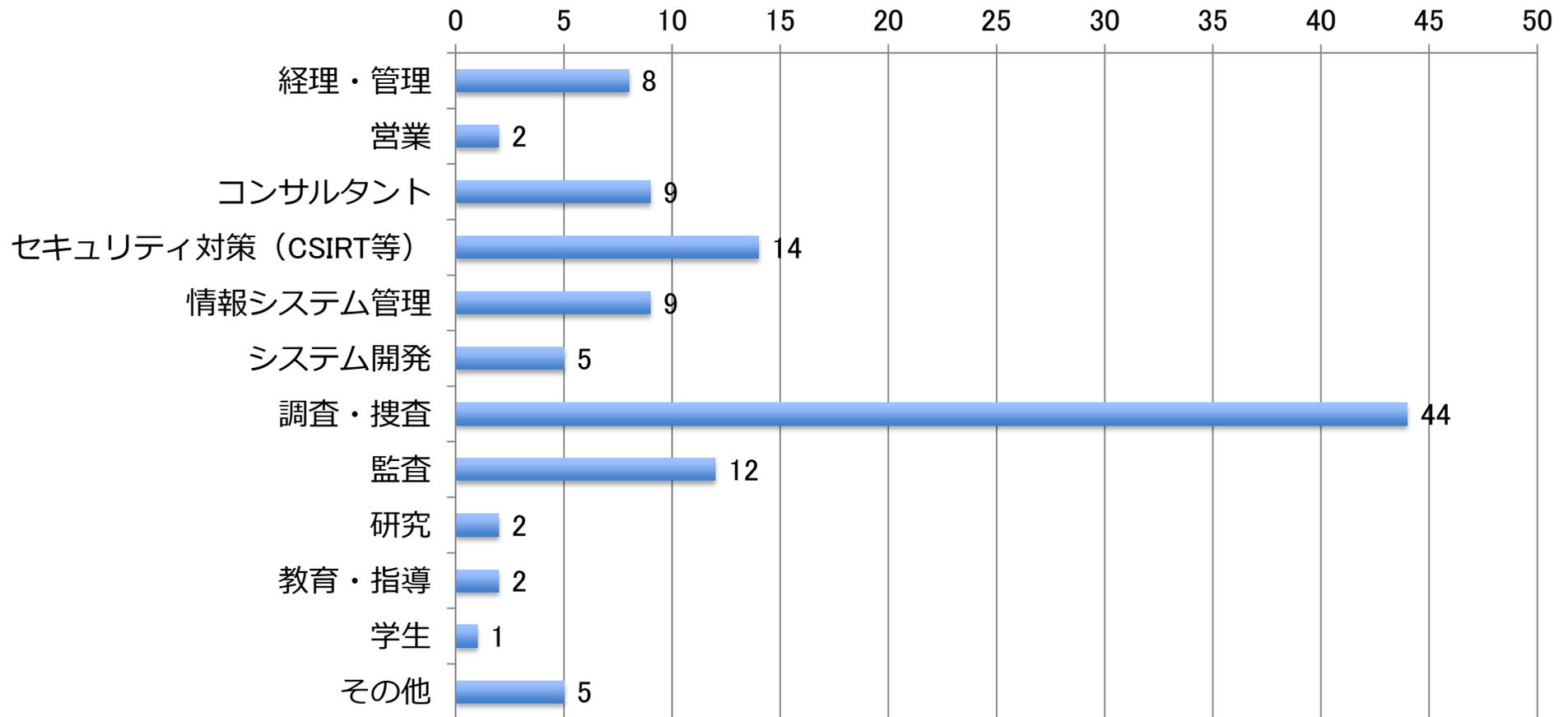


参考：デジタル・フォレンジック・コミュニティ2017参加者の所属組織



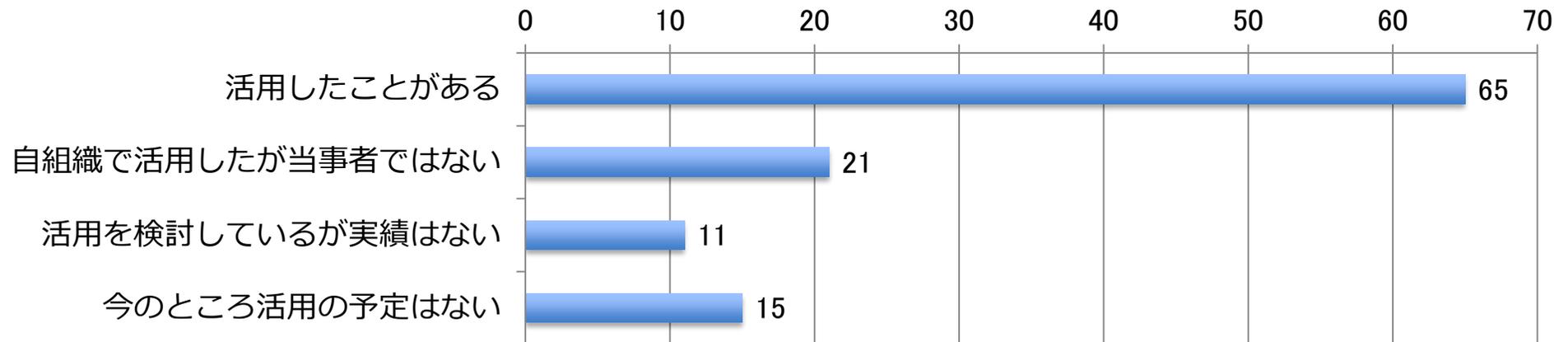
2.2. ご自身の現在の立場を教えてください

(1つだけ選択)



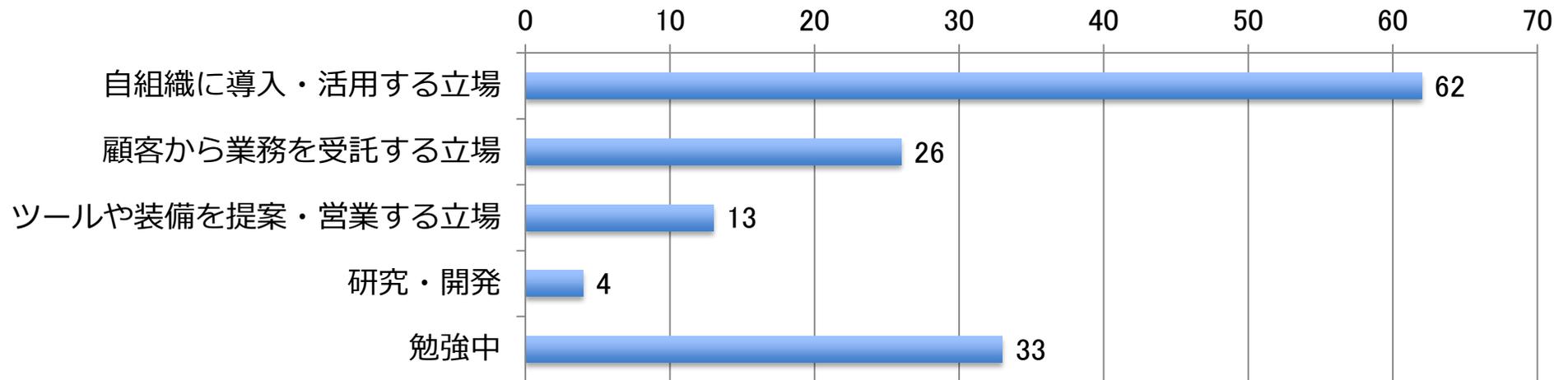
2.3. デジタル・フォレンジックの活用経験は？

(1つだけ選択)



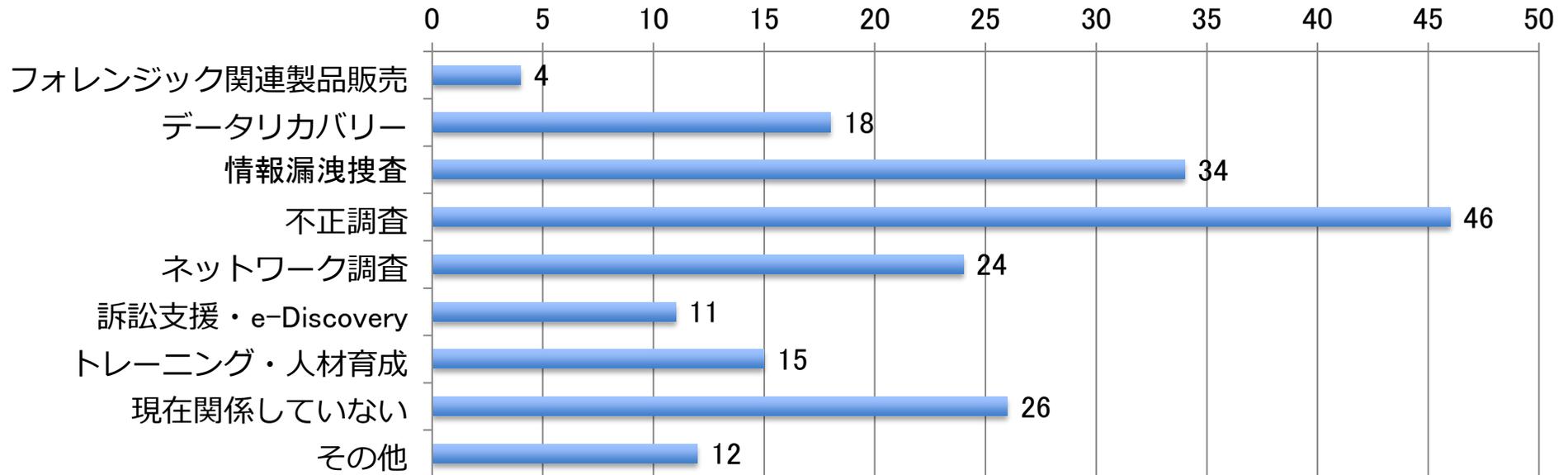
2.4. ご自身が「デジタル・フォレンジック」に関わる立場を教えてください

(複数回答可)



2.5. 現在関係している「デジタル・フォレンジック」の分野は？

(複数回答可 + 自由記入)

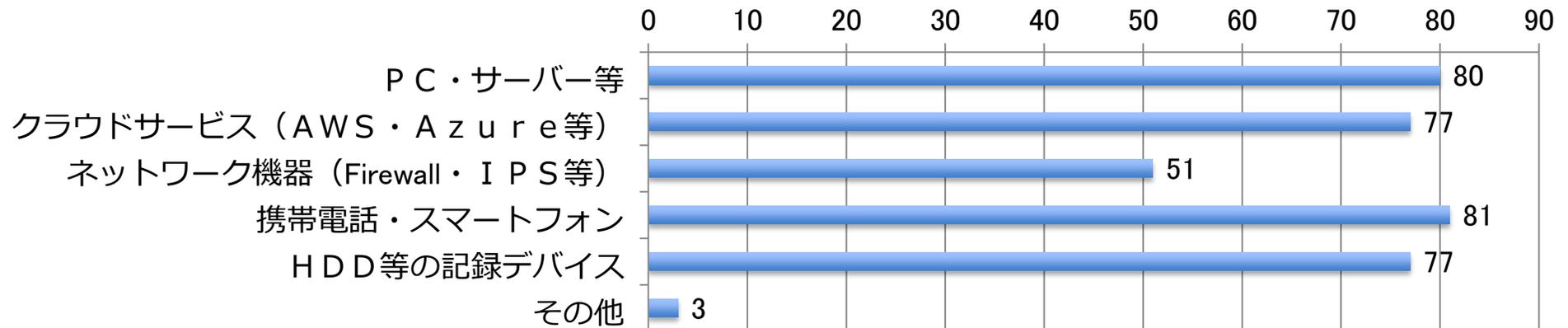


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（+）反対票（-）

- 犯罪捜査 +40
- インシデントレスポンスファストフォレンジック +18
- モニタリングに活用したい +10
- デジタル遺産 +4
- 大学でデジタル・フォレンジックを研究しています +6
- データをゴリゴリほじくりだしてます。 +3, -2
- デジタル遺産って何？ -1

2.6. 「デジタル・フォレンジック」の対象として思い浮かぶものは？

(複数回答可 + 自由記入)

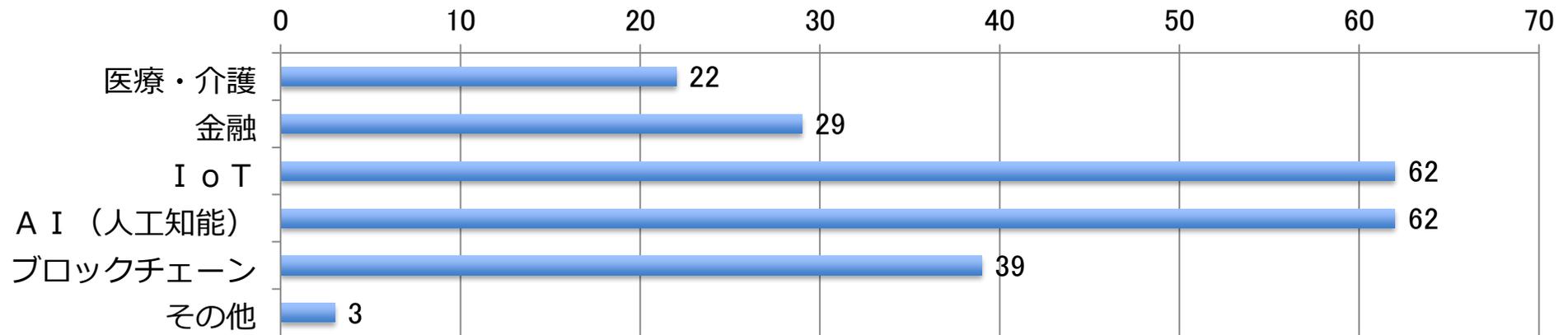


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票 (+) 反対票 (-)

- IoTデバイス +31
- 家電 +13
- 今後スマホは厳しいっすよね~? +13, -2
- 防犯カメラ +12
- 自動車関連 +10
- 交通事故におけるデジタルフォレンジック +9
- ゲーム機 +7, -1
- 生体認証デバイス +5
- スマートゲートウェイ 4
- SEIM +4
- スマートキー
- 監視カメラ
- 入退出記録

2.7. 最も有望なビジネス分野はどこですか？

(複数回答可 + 自由記入)

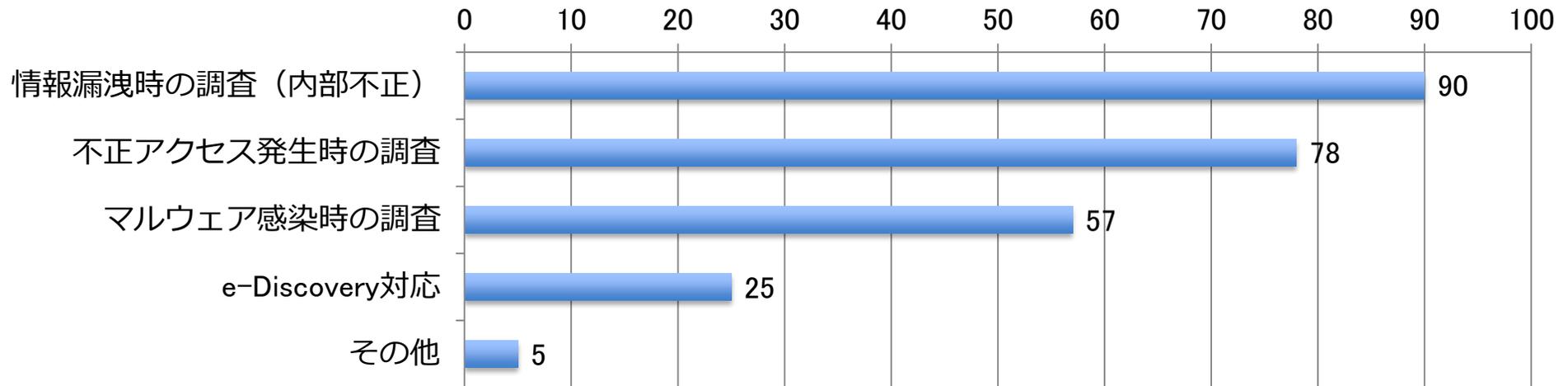


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（+）反対票（-）

- 2020オリパラ +22, -1
- 大阪万博！！ +9
- 物流 +7
- 自動車関連 +5
- デジタルガバメント +5, -1
- 航空宇宙分野 +3
- 訴訟対策 +2, -1
- 購買 +2, -1
- HEMS -1

2.8. 「デジタル・フォレンジック」の有益な活用分野はどこですか？

(複数回答可 + 自由記入)

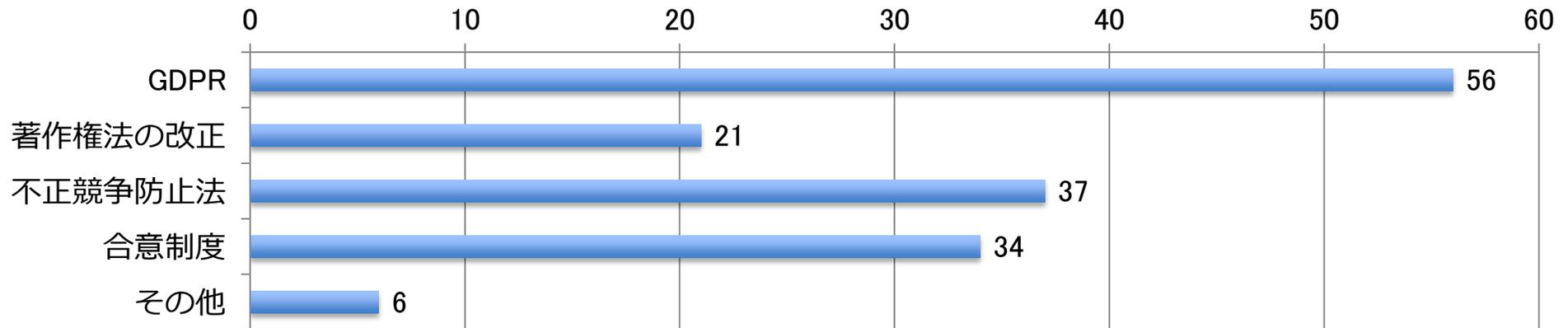


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票 (+) 反対票 (-)

- R P A +9, -1
- 公判対策 +6
- ロボティクスオートメーション +2
- 不倫調査 +1, -1
- 犯罪捜査におけるデジタル証拠品解析
- 米国 Cloud Act

2.9. デジタル・フォレンジック分野に影響を及ぼす国内外の法改正は？

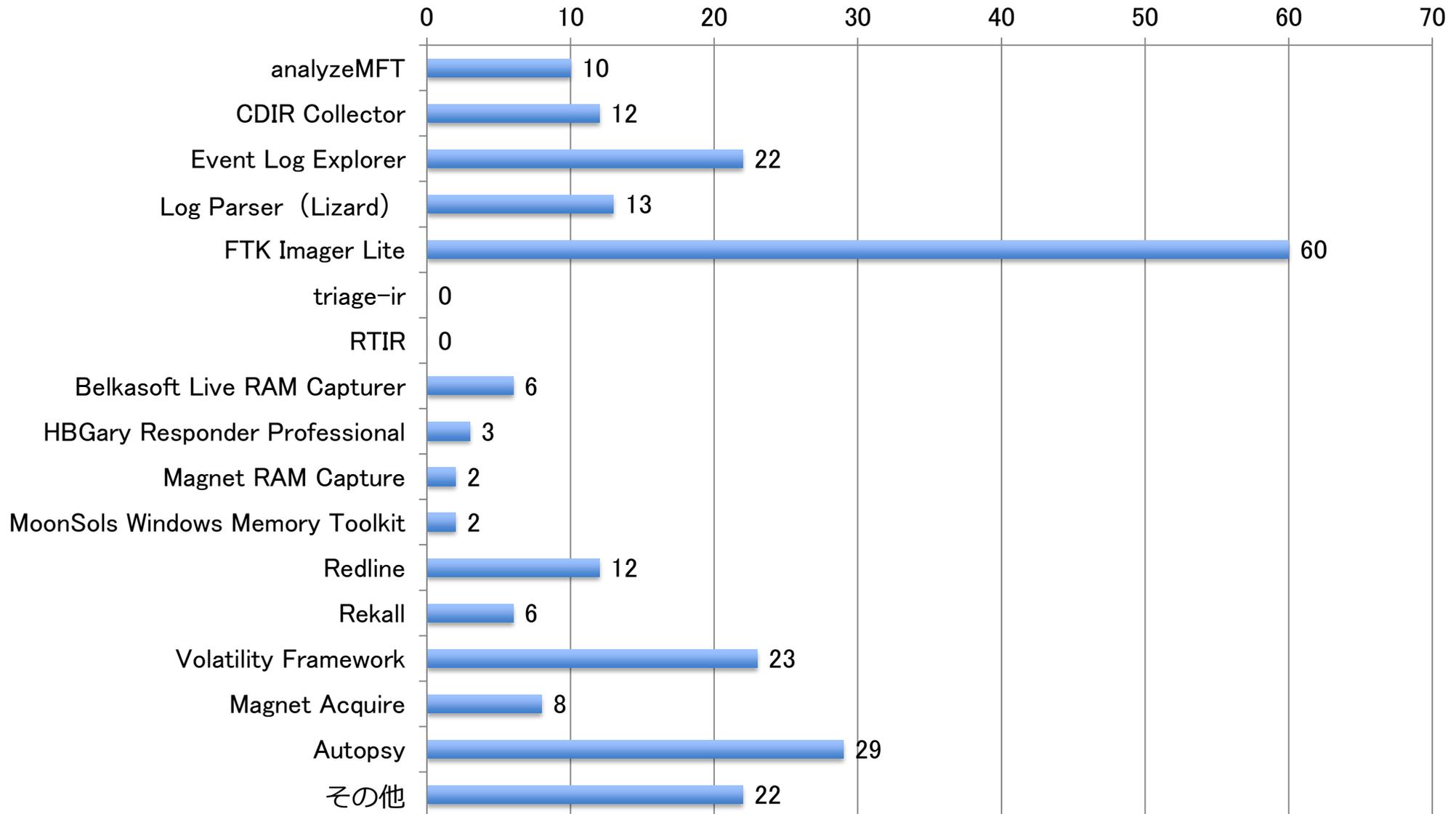
(複数回答可 + 自由記入)



●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（+）反対票（-）

- 入管法 +19
- 法じゃないけど来年の年号 +7
- サイバーセキュリティ法(中国) +6
- プライバシー +5
- 合意制度は未知数かな。 +1

2.10.1 使ったことのあるツールを教えてください（複数回答可）

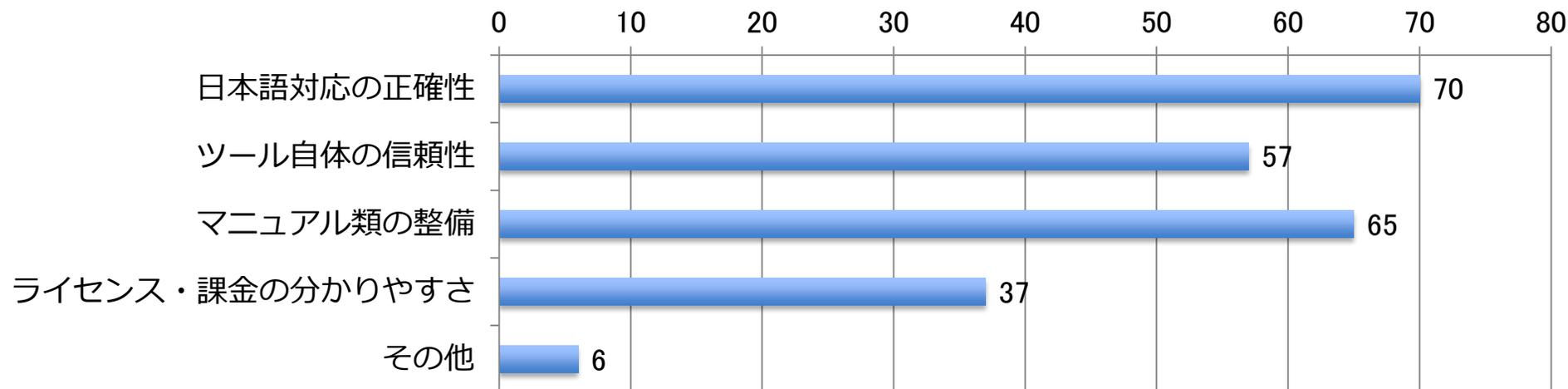


2.10.2 使ったことのあるツールを教えてください（自由記入）

- 自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（+）反対票（-）
 - EnCase +23
 - FTK +17
 - ユーフェド +15
 - Oxygen +14
 - IDA Pro +9
 - 使ったことがない +7
 - AXIOM +6
 - SANS SHFT +6
 - DEFT +5
 - nuix +4
 - 剣 Linux +2
 - 蟹reg +1
 - FF
 - plaso
 - Email Auditor
 - Falcon
 - Lit i view

2.11. 海外ツールを使用する際の課題や問題点は？

(複数回答可 + 自由記入)

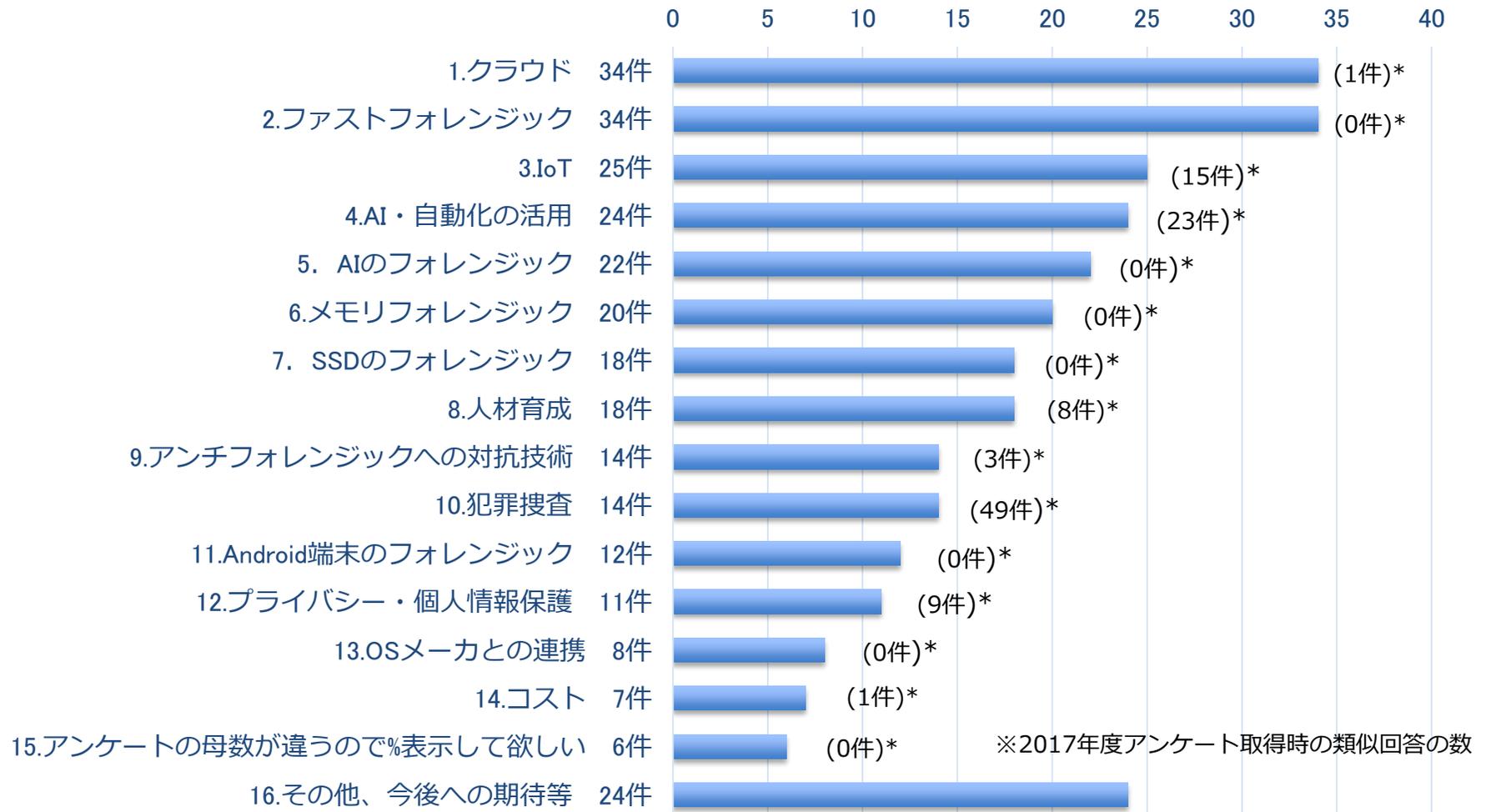


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（+）反対票（-）

- 日本語に限らず文字コードの対応 +10
- マニュアルのマニュアルが必要 +10, -1
- クラウド環境 +8
- フリーツールでもどういう許諾条件かわからなかったりする +7
- 公判対応 +6
- サポート +6
- 自分の英語力 +5, -1
- ベンダー経由だと高い +5, -1
- 使ったことないのでわかりません +3, -1
- ユーザーコミュニティ +2
- 使ったことがない +2, -1

2.12.1. 「デジタル・フォレンジック」に期待する分野・方向性、 今後の調査項目等について（自由記入内容の取りまとめ結果）

- 下記の棒グラフはアンケートに回答した自由記入コメントを類似項目で集約し「賛同票」を加算したものである。
（反対票数の減算はしていない）
類似のコメントが4件以下のコメント（7項目）はその他に分類した。



2.12.2. 「デジタル・フォレンジック」に期待する分野・方向性、 今後の調査項目等について 1/2

(自由記入内容)

- 1.クラウド 34件
 - ・クラウドの調査 +20
 - ・クラウド +12
- 2.ファストフォレンジック 34件
 - ・ファストフォレンジック +15, -1
 - ・ファストフォレンジックを証拠保全の観点から見直さないといけないと思います。 +5, -1
 - ・ファストフォレンジックに必要な事前のセキュリティ設定 +11
- 3.IoT 25件
 - ・IoT +14
 - ・IoT機器の解析手法 +9, -1
- 4.AI・自動化の活用 24件
 - ・フォレンジックのある程度の自動化 +13
 - ・データアナリティクス・予兆検知・リスクシナリオ +2
 - ・デジタル・フォレンジックにおけるA Iの活用
 - ・非構造化データのモニタリング高度化 +4, -1
5. AIのフォレンジック 22件
 - ・AIのフォレンジック +21
- 6.メモリフォレンジック 20件
 - ・メモリフォレンジック +19
7. SSDのフォレンジック 18件
 - ・SSDのフォレンジック・新たな暗号の規格や実装 +17
- 8.人材育成 18件
 - ・フォレンジックエンジニアの給与水準 +8
 - ・官民の更なる連携（特に人材育成、人材確保） +8
- 9.アンチフォレンジックへの対抗技術 14件
 - ・アンチフォレンジックへの対抗技術 +13
- 10.犯罪捜査 14件
 - ・犯罪捜査の不正アクセス防止法からの解放 +13, -1
- 11.Android端末のフォレンジック 12件
 - ・Android端末のフォレンジック +11, -1
- 12.プライバシー・個人情報保護 11件
 - ・暗号化、プライバシーと証明、証拠のジレンマ +9
 - ・個人情報を含む秘密情報の保護の強化、透明化に関する技術提供
- 13.OSメーカーとの連携 8件
 - ・フォレンジックの肝はOSなのでOSメーカーの見解しりたい +7
- 14.コスト 7件
 - ・コスト +6, -1
- 15.アンケートの母数が違うので%表示して欲しい +5, -1
- 16.その他、今後への期待等 24件
 - ・海外サーバの法的 +4
 - ・作業の標準化 +4, -1
 - ・リアルタイムで結果が見られるアンケート、楽しいです。 +4, -1
 - ・限界領域 +3
 - ・日本経済の発展 +2, -2
 - ・産業として発展するように願っています -1
 - ・安全保障

3. 考察と今後の取り組み（案）

1. 調査手法について

- 2018年度は2017年度に引き続き、コミュニティのプログラムとして20分間確保し、WG主査が壇上から設問の解説やリアルタイムに表示されるアンケート結果への寸評を加えつつ、オンラインアンケートシステムを活用して、大きなトラブルなく実施することが出来た。
- スマホやパソコンのWEBブラウザを利用したオンラインアンケートシステムは、リアルタイムでアンケート結果が表示され他人の意見がその場で共有されるため、来場者の意見を引き出す有効な手段と思われる。
- しかし、スマホ等によるアンケート回答が馴染まない来場者が一定数おり、より多くの来場者にアンケートに協力していただくためには、紙アンケートとの併用が必要であり、今後は重複カウントしない配慮をしつつ、オンラインアンケートと紙アンケートを併用して行うこととしたい。

2. 回答内容の分析について

- 2018年度のアンケート項目は2016年度からの実施結果を踏まえて、追加変更しており、単純に経年変化の比較をできないが、デジタル・フォレンジックの活用分野（情報漏洩・不正アクセス・マルウェア感染）には大きな変化はない。
- 一方で、自由記入していただいた「2.12.2. デジタル・フォレンジックに期待する分野・方向性、今後の調査項目等について」の結果は、昨年と順位が入れ替わっており、クラウドのフォレンジックやファストフォレンジックに多くの参加者が興味を持つまたは期待していることが伺われる数値が得られた。
- 2018年度に新たに追加した「国内外法制度の影響」や「海外フォレンジックツールの評価」については、関心の高さが伺える回答を得ることが出来たことから、2019年度も継続して調査していきたい。

3. 今後の取り組み

- 2018年度も2017年度に引き続き、自由記入コメントに多岐にわたる意見が寄せられたことから、2019年度も来場者に落ち着いて記入していただける時間配分等に配慮していきたい。
- 2018年度調査結果の報告会を開催するとともに、調査結果はIDFのWEBサイトで公開することとする。