2019年度
デジタル・フォレンジック
普及状況調査結果

2020年3月

DF普及状況調査WG

目次

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

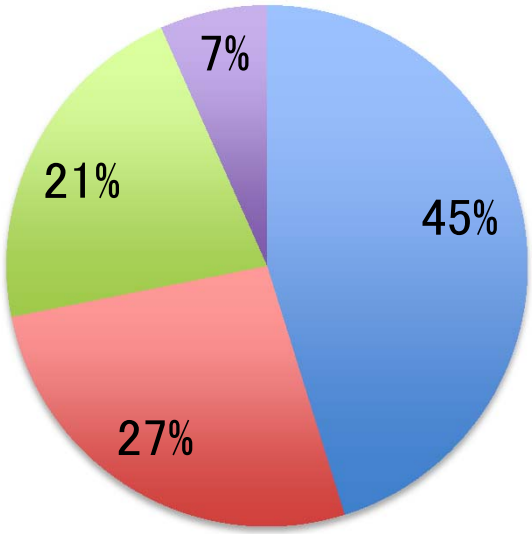
2019年度の調査では、前年度と同様にコミュニティ2019のセミナープログラムに「30分間のWEBアンケート」を設けて実施し、WEBアンケートと紙アンケートを併用し137名の協力を得ることができた。

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。

2018年から調査項目に採用した、デジタル・フォレンジック製品（ツール）の利用状況の調査では、59製品の名称と製品概要をリスト化し、会場の参加者に配布したうえでWEBアンケートを行うなど、短時間で多数の回答を得るための工夫したこともあり、多数の回答を頂けた。

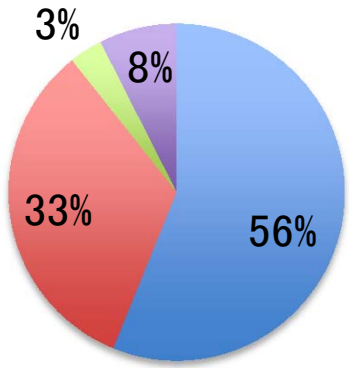
アンケートにご協力いただいた皆様に御礼を申し上げます。

2.1. ご自身の所属組織を選んでください

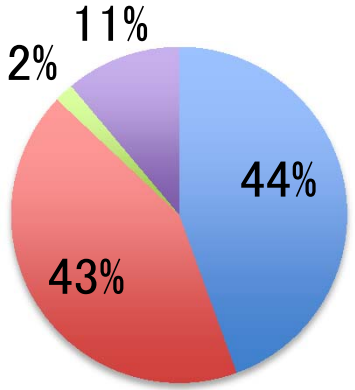


- 民間企業（61）
- 行政機関（36）
- 大学・研究機関（29）
- その他（9）　※ 再掲：法執行機関2名

コミュニティ2017参加者

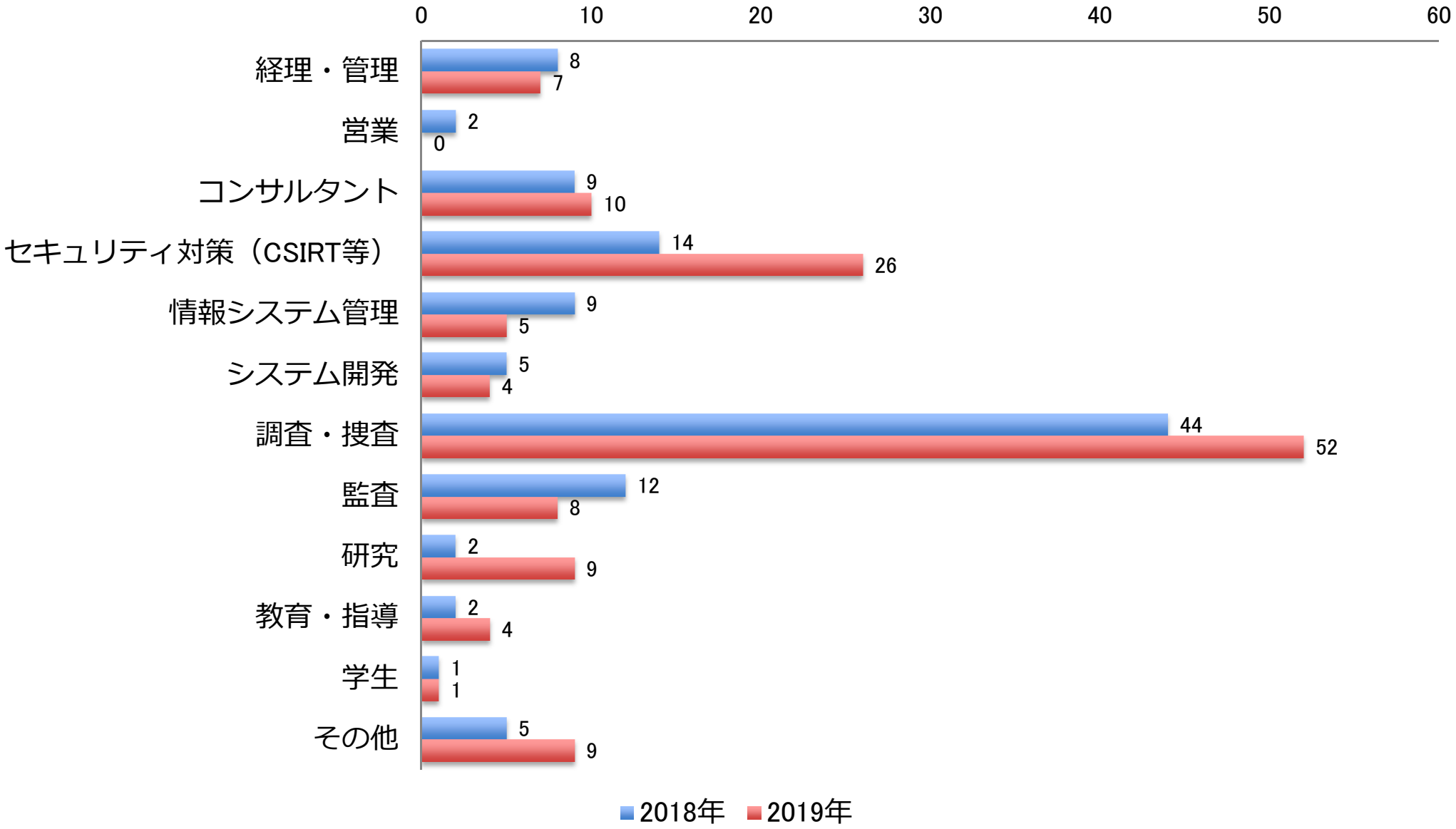


コミュニティ2018参加者



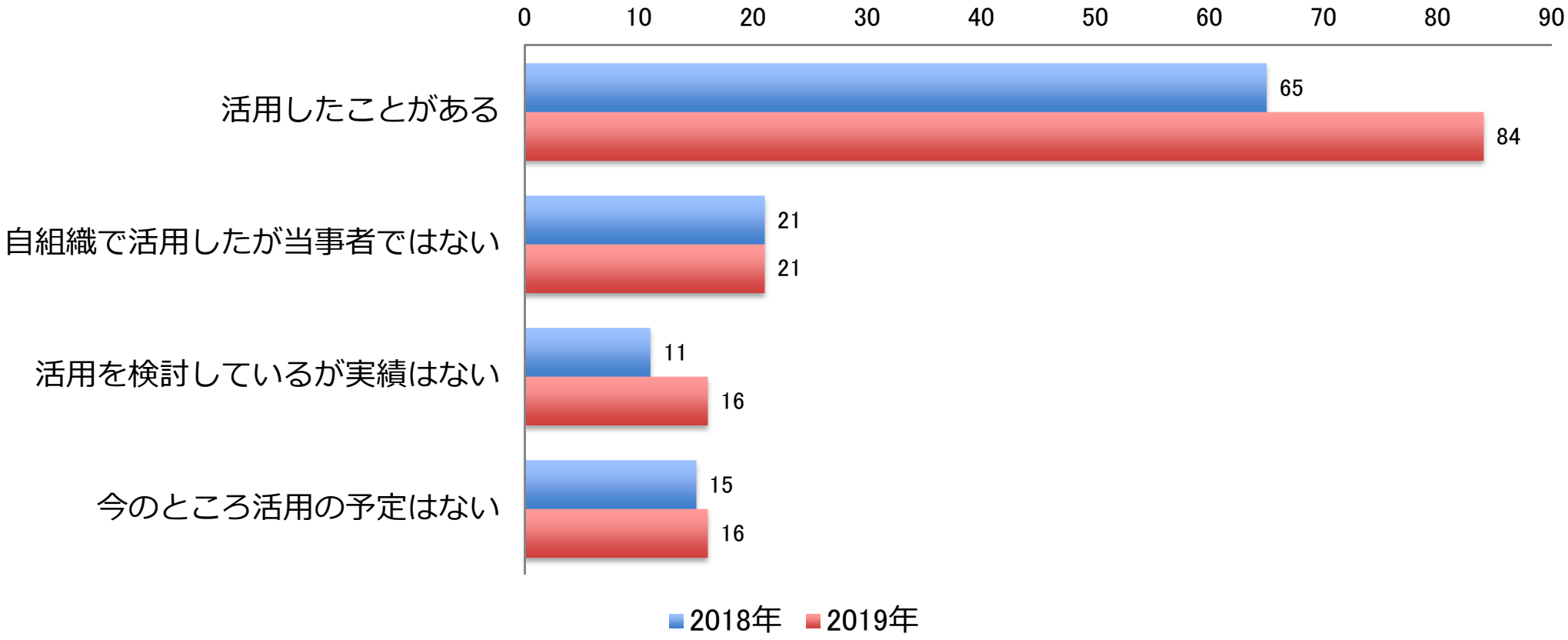
2.2. ご自身の現在のお仕事を選んでください

（１つだけ選択）



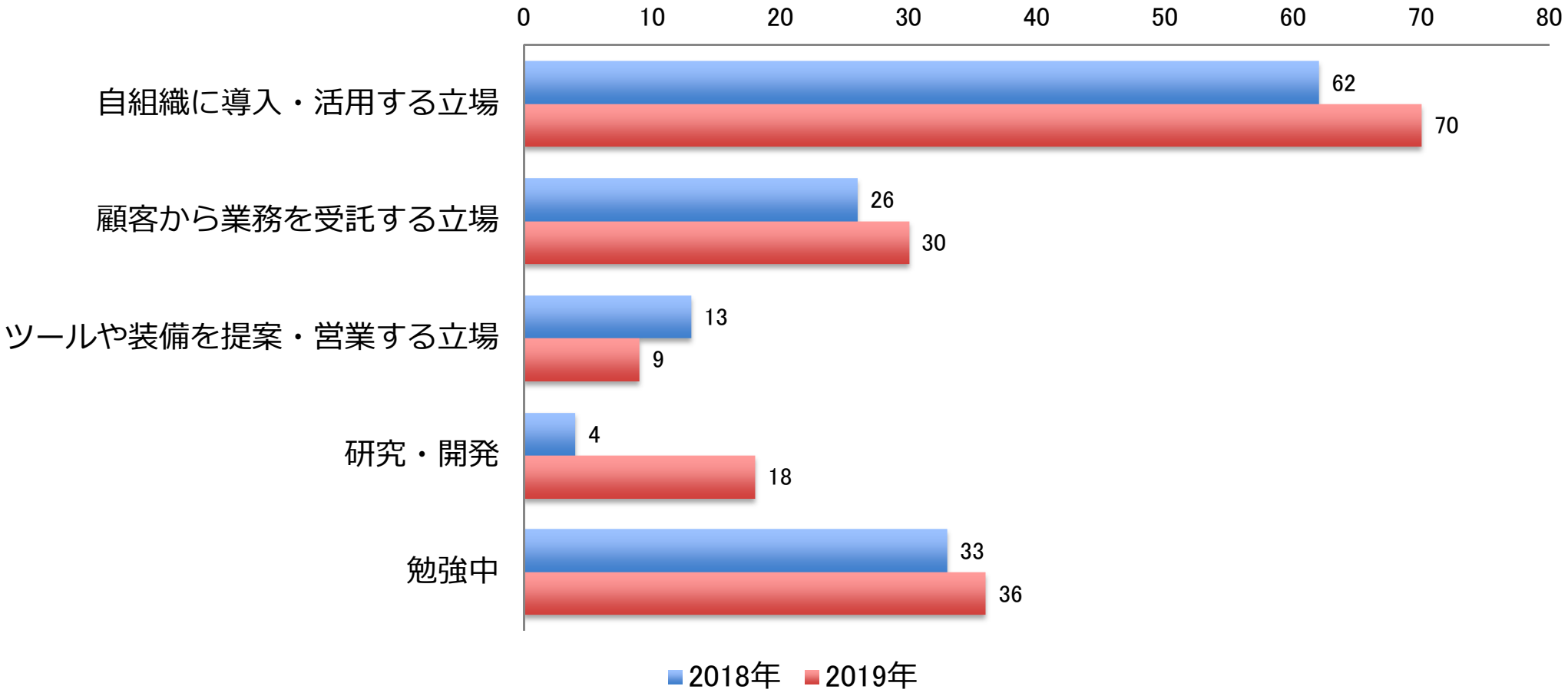
2.3.デジタル・フォレンジックの活用経験は？

（１つだけ選択）



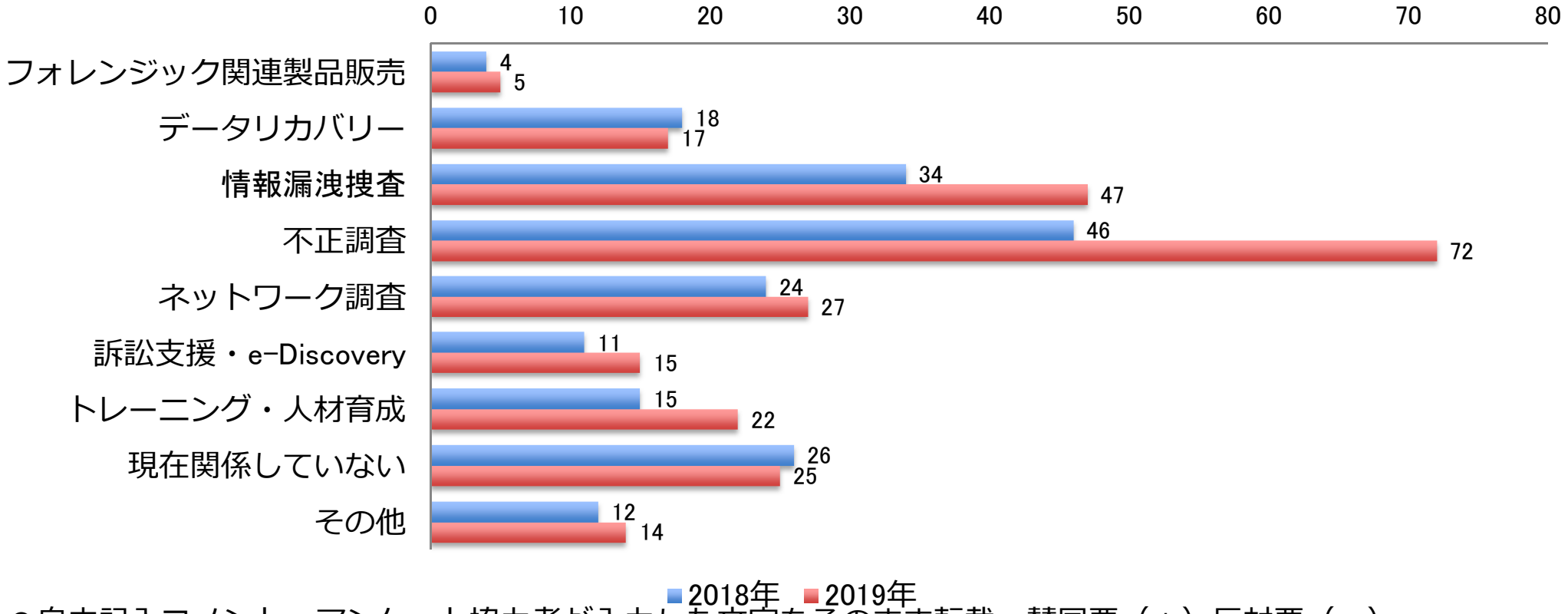
2.4. ご自身が「デジタル・フォレンジック」に関わる立場を教えてください

（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）



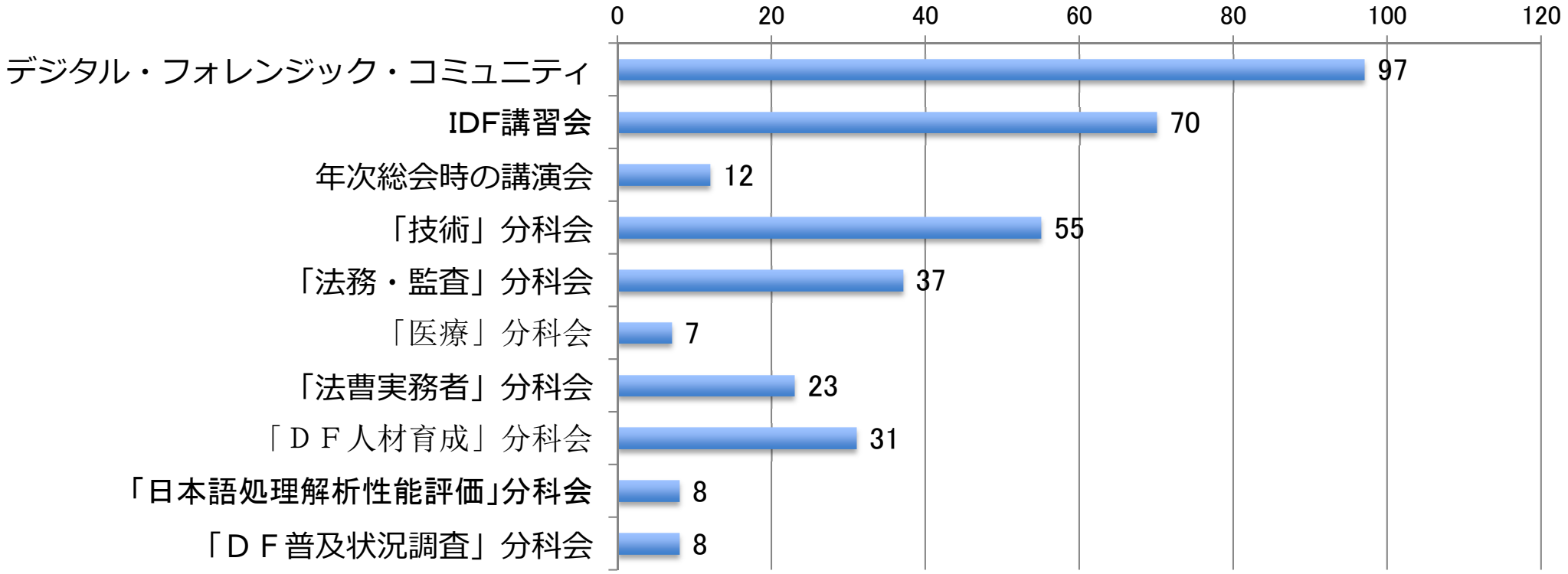
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【 2018年】
- 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

【 2019年】
- 犯罪捜査 +9
- 解析結果を証拠として見て判断する側
- データ解析・機器修繕
- 研究

2.6. デジタル・フォレンジック研究会の活動で参加してみたいものは？

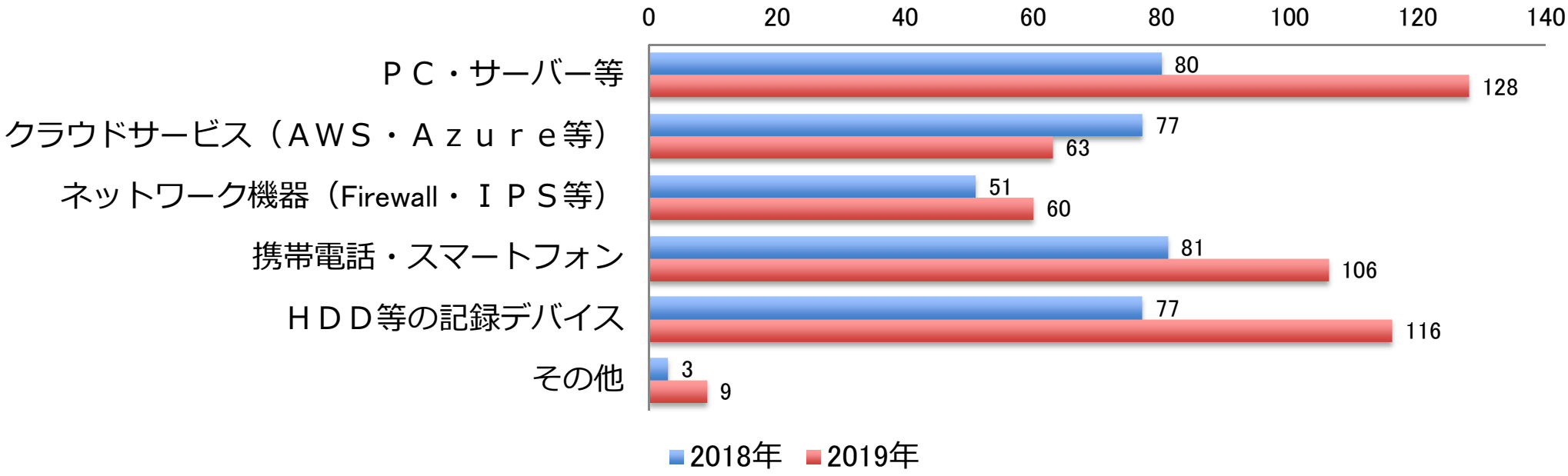
（複数回答可）



※ この設問は2019年から新しく採用

2.7. 「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）



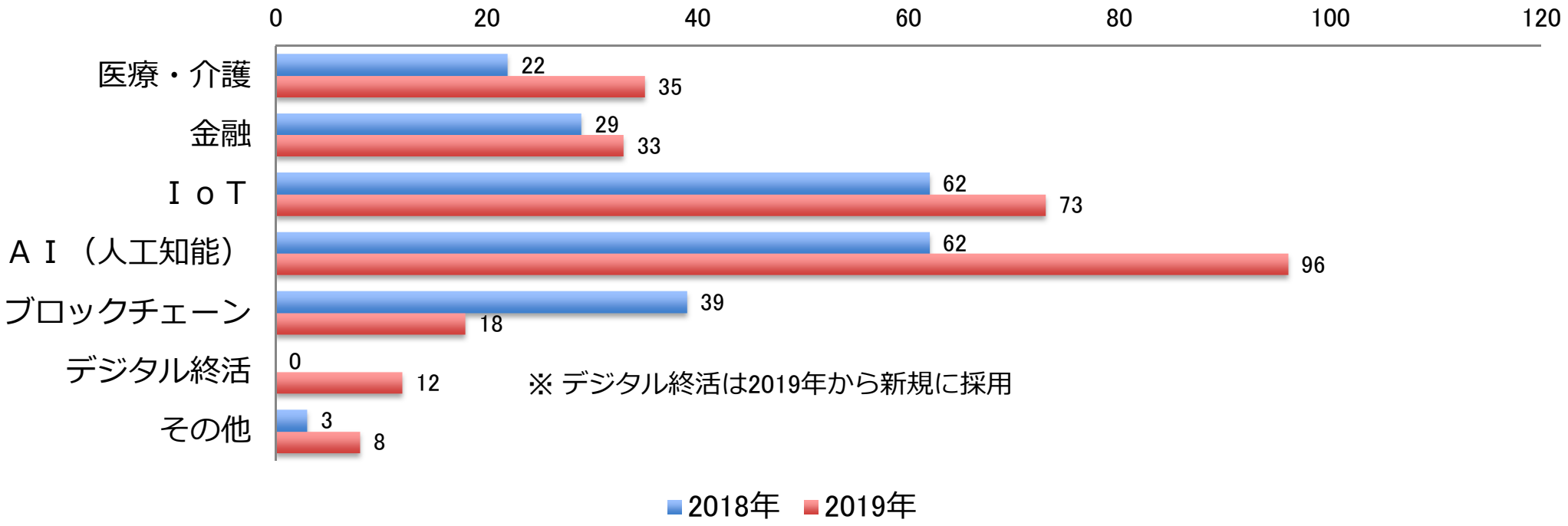
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【2018年】
- 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

【2019年】
- ドライブレコーダー　+5
- メモリ　+3
- IoT機器　+1
- 本
- 人

2.8. 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）



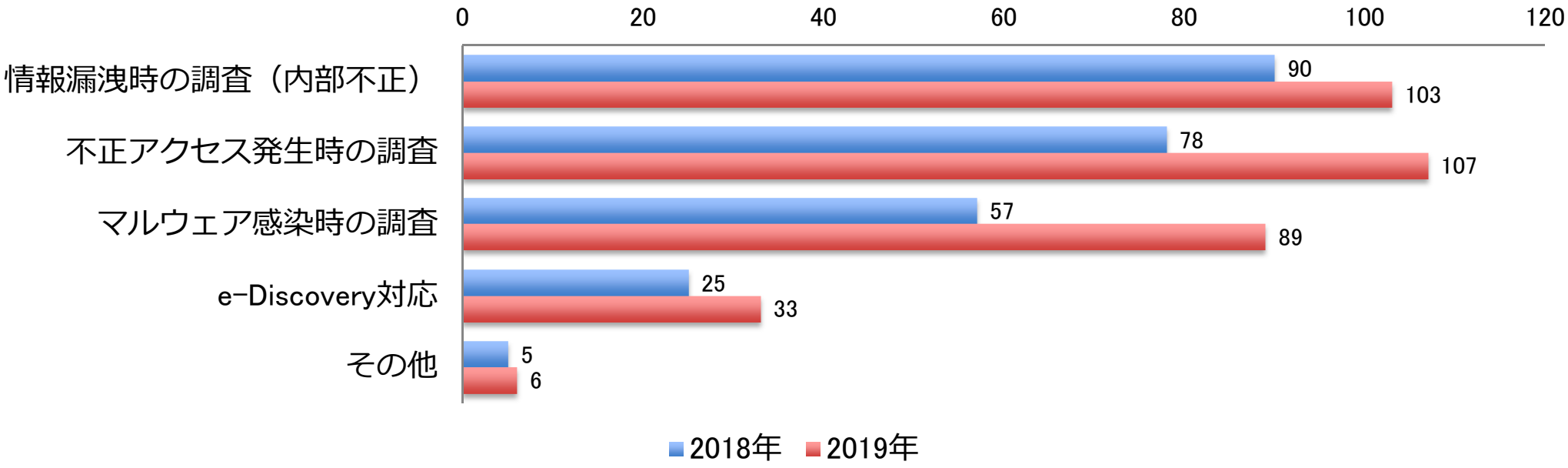
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【2018年】
- 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

【2019年】
- 物流　+3
- VR
- ODR（特に，行政機関との連携もできれば爆発すると思う）
- コンテンツ管理
- ドローン等情報収集用遠隔操作機器
- マッチングサービス、自動運転
- 民事紛争

2.9. 「デジタル・フォレンジック」の有益な活用目的はどこですか？

（複数回答可＋自由記入）



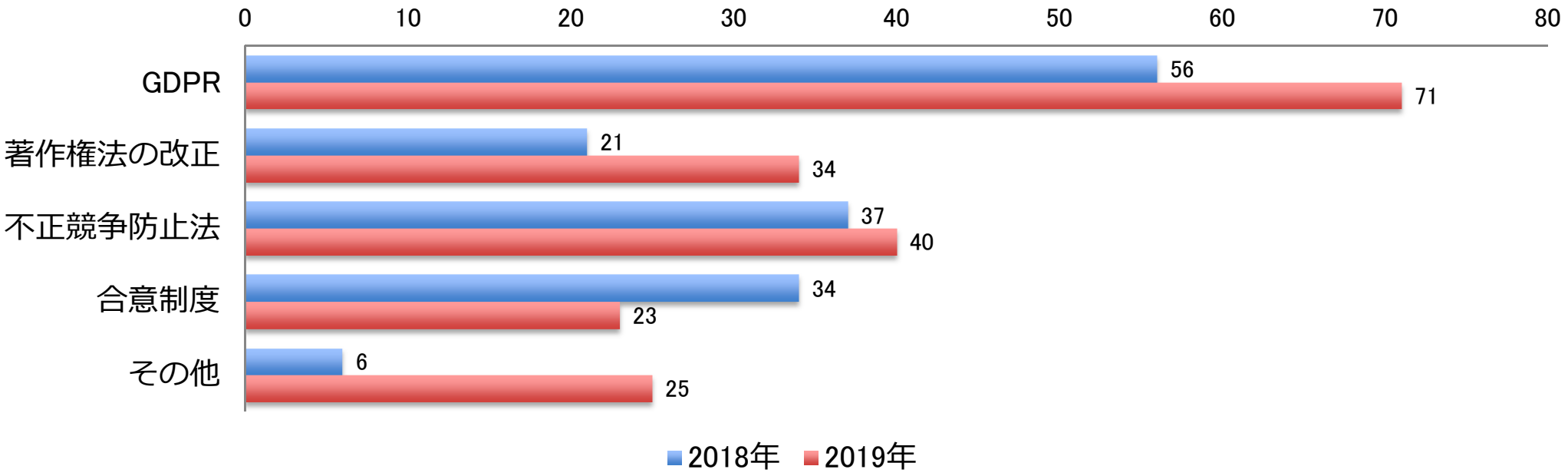
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【2018年】
- ＲＰＡ　+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

【2019年】
- パワハラ・セクハラ調査　+7
- 犯罪捜査

2.10. 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令は？

（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（ー）

【2018年】
- 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

【2019年】
- 不正アクセス禁止法　+14
- 刑事訴訟法　+10　-1
- 通信の秘密(電気通信事業法)　+7
- ウィルス作成罪　+7
- 民事訴訟法　+3
- 労働基準法(ブラック企業調査)　+2
- 民法　+1
- 電波法　+1
- 刑法　+1
- 国際法　+1　-1
- サイバー犯罪条約
- 会社法
- 通信傍受法
- 米国CLOUD法
- 海外サーバの差押え、保全
- 個人情報保護法
- 通信傍受の規則、文化監修、認知の歪み

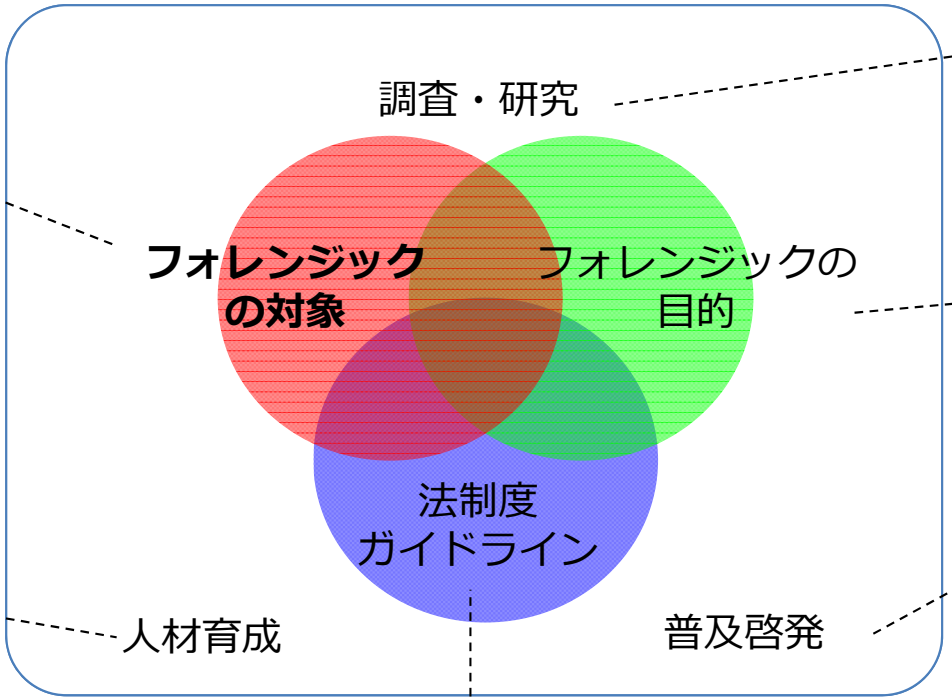
2.11 使ったことのあるツールを教えてください（複数回答可）

製品名	投票数	製品名	投票数
1. Autopsy	36	31. Magnet RAM Capture	7
2. AXIOM/IEF [Internet Evidence Finder](Magnet Forensics)	25	32. Magnet Acquire	7
3. Arsenal Image Mounter	4	33. MSAB Office	9
4. analyzeMFT	12	34. Net Hunter	0
5. Belkasoft Evidence Center(Belkasoft)	15	35. Nuix Workstation	6
6. BlackLight / MacQuisition (BlackBag)	17	36. Nuix Investigate	10
7. Cain	18	37. Nuix Discover	3
8. CDIR Collector（Cyber Defense Institute Incident Response Collector）	25	38. Oxygen Forensic Detective	22
9. DEFT（Digital Evidence＆Forensics Toolkit） DART（Digital Advanced Response Toolkit）	17	39. PassWare Kit	17
10. Email Auditor 19（メール監査ツール）	5	40. PC-3000	11
11. EnCase (OpenText)	72	41. Phone Breaker (Elcomsoft)	0
12. Eric Zimmerman ツール	11	42. Paladin Linux / RECON(SUMURI)	3
13. Event Log Explorer	22	43. Plaso	11
14. Final Forensic / AndrEx (AOS)	15	44. RECON IMAGER	2
15. F-Response	0	45. RECON LAB	3
16. FTK [Forensic Tool Kit] (AccessData)	58	46. Redline	9
17. FTK Imager Lite , FTK Imager	81	47. Rekall	9
18. Ghidra (NSA)	8	48. Responder Pro	4
19. Griffeye	0	49. SIFT Workstation (SANS)	15
20. HX-Recovery for DVR & NVR	0	50. Simple SEIZURE TOOL for Forensic (SSTF)/for Android (SSTA)	9
21. IDA Pro (Hex-Rays)	29	51. Splunk	33
22. Intella	6	52. Tsurugi (剣) Linux	14
23. Kansa	5	53. TZWorks (の各種パーサー)	4
24. KIBIT Automator（AIツール）	2	54. UFED 4PC (Cellebrite)	33
25. Kali Linux	54	55. UFED Mobilogy　Touch	15
26. LACE	0	56. VFC5（Virtual Forensic Computing）	8
27. Lit i View E-DISCOVERY(データ解析ツール)	6	57. Volatility Framework	35
28. Lit i View XAMINER(データ解析ツール)	20	58. VizX (Ziuz)	0
29. Log Parser（Lizard）	13	59. X-Ways Forensics	42
30. MacQuisition	11	※製品概要は別紙参照	

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）

●自由記入アンケートで得たコメントを、フォレンジックの対象、フォレンジックの目的、法制度・ガイドラインなどに分類して整理を試みた。今後はこれら課題解決に向け取り組みが進むことを期待したい。

【期待する分野・方向性の分類】



フォレンジックの対象（＋187,-2）
暗号化されたファイル、クラウドデータの復元、SSDやメモリ、AIなどを対象とした分野

調査・研究（＋23）
フォレンジック関連の証拠能力及び証明力の理論的・実証的研究、ライブフォレンジックの証拠価値、研究促進の為の研究データセット提供等

フォレンジックの目的（＋70）
ファストフォレンジックと証拠化手続き、画像改竄、アンチフォレンジックの発見、トリアージ等の分野

人材育成（＋39）
フォレンジック特化CTF、人材育成ガイドライン、技術をどう身につけていくか、初心者でも簡単に学べる環境づくり等

普及啓発（＋46,-3）
法執行機関専用のコミュニティの開催、日本語に対応したフォレンジック解説サイト、内容をマスク化して案件共有したい等

法制度・ガイドライン（+21, -1）
ログ保存期間やフォレンジックを想定した設定の普及、フォレンジックや各種解析に対応した令状及び法制度の形成、国内外問わず法体系の課題抽出及び提言等の方向性

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．フォレンジックの対象（＋187,-2）

- 暗号化されたファイルをどうするか　+29

- クラウドデータの復元　+21
- クラウド上に分散管理されているデータの収集　+15
- AWSやAzureのフォレンジック　+8 -1
- クラウドへのアクセス　+6
- リモートのフォレンジック　+11

- SSDの復元　+15
- メモリフォレンジックへの対応(Volatilityが最新のOSに追いついていない等)　+4

- AIへの対応　+7
- AIへの攻撃　+2

- シンクラ対応　+8
- MacとLinuxのフォレンジック　+7
- T2チップ搭載のMac　+7

- ノートPCが増えWiFiを切る指令をだすとPCのシャットダウンがされて、メモリが読めない　+3 -1
- 公衆無線LAN　+4

- 車のフォレンジック　+16
- ドローンの飛行歴　+6
- IoTのセキュリティ対策

2．フォレンジックの目的（＋70）

- ファストフォレンジック　+12
- ファストフォレンジック結果の刑事事件における証拠化手続き　+11
- 多数端末に対するファストフォレンジック　+6
- ファストフォレンジックにおける推認過程の理論化・定式化　+4

- 画像改竄　+7

- アンチフォレンジックの発見　+4
- トリアージ+4
- デジタル・フォレンジックの事例分析から鑑みた不正検知+4
- 音声記録を含めた不正調査の効率化+3

- e-discovery　+2
- e-disを見据えたインフラ構築(バックアップ、暗号化)　+1

- SVのバックアップを取っても容量Overに陥ってしまう

3．法制度・ガイドライン（+21, -1）

- ログをある程度の期間残すなど、フォレンジックを想定した設定の普及　+7-1
- フォレンジック，各種解析に対応した令状及び法制度の形成　+4
- 違法なデータがフォレンジック後に抽出された場合　+3
- 国内外問わず法体系の課題抽出及び提言　+2
- フォレンジック関連の法整備・クラウド、パスワード解除・暗号化ファイルの復号

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　2/2

（自由記入内容）

4．調査・研究（+23）
- フォレンジック関連証拠の証拠能力及び証明力の理論的・実証的研究+9
- フォレンジックを行うことによる情報漏洩リスク6
- ライブフォレンジックの証拠価値+3
- 研究促進の為の研究データセットのご提供+1

5．人材育成（+39）
- フォレンジック特化CTF　+10
- 人材育成ガイドライン　+8
- 人材育成　+8
- 技術をどう身につけていくか+7

- 案件のマネジメント能力(ノンテク)の向上
- 初心者でも簡単に学べる環境づくり

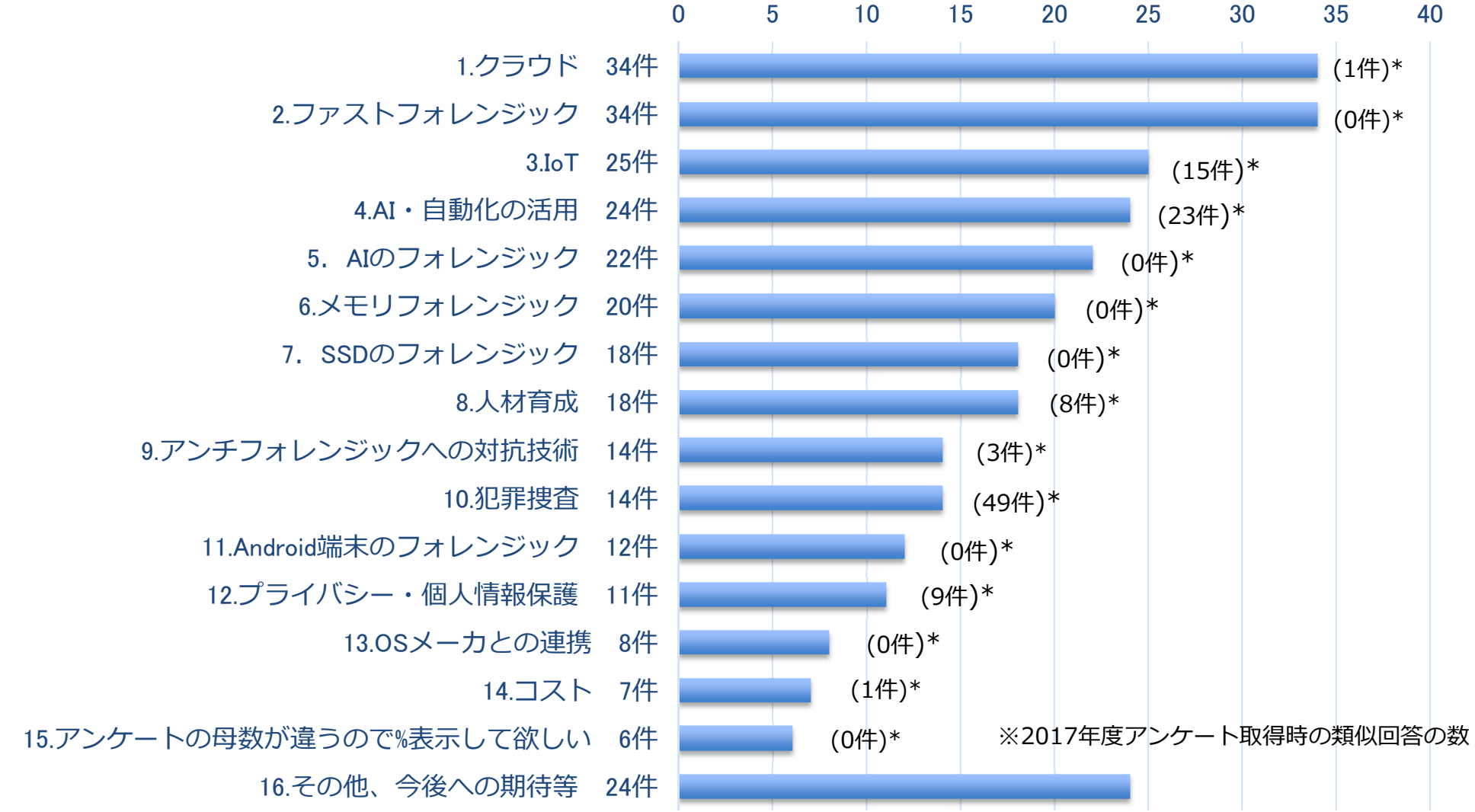
6．普及啓発（+46,-3）
- 法執行機関専用のコミュニティの開催　+10
- 相当の勉強を必要としないツールがほしい　+9 -2

- 犯罪捜査では先行しているようですが、民間企業での活用が期待されると思います　+5
- フォレンジック技術を通じ，証拠保全とその過程の重要性が深く認識されるようになってほしい　+4
- 内容をマスク化して、案件共有したい　+3
- 日本語に対応したフォレンジック解説サイト　+3
- 利用者側への理解　-1
- インシデント対応に対する考え方（事故を起こした社員を複数人で責め立てるのを止めるなど）　+1
- 民間企業での使用
- 今後のフォレンジック調査方法について
- 不正への“ケンセイ”となるような事例の広報や周知（不正が割が合わないと思いととらせるようなフォレンジックの活用効果）

7．その他（+10,-1）
- ツール一覧大変参考になります。価格も載せていただけますとなおありがたいです　+4
- 法執行機関に対するバックドア　+4-1

参考：2018年 「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）

●下記の棒グラフは自由ンケートに回答した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。



参考：2018年 「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）

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ＡＩ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

- 2019年度はコミュニティのプログラムとして（30分間確保）、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、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、来場者の気付きや意見を引き出す有効な手段と思われる。
- 今年はスマホ等によるアンケート回答が円滑に行われ、80名程度の来場者がWebアンケートに協力いただき、会場の雰囲気も良くかなりの盛り上りを見せた。また昨年同様に紙アンケートとの併用を行ったため、137名もの回答を得ることができた。今後も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

- 2019年の回答内容は2018年度と比較しても、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、デジタル終活等の新しい分野の動向を見守りたい。
- 昨年同様に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回答が得られた。
- フォレンジックツールの利用状況調査は、多くの回答を得ることが出来たことから、2020年度も継続して調査するとともに、IDF会員への有益な情報提供に繋げていきたい。

4. 今後の取り組み

- 2019年は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。
- 2019年度調査結果はIDFのWEBサイトで公開することとする。