2020年度
デジタル・フォレンジック
普及状況調査結果

2021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分野において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

2020年度の調査では、前年度と同様にコミュニティ2020のセミナープログラムに「30分間のWEBアンケート」を設けて実施した。WEBアンケートに参加した方が48名、事前のアンケートの回答者が14名、合計で62名の協力を得ることができた。

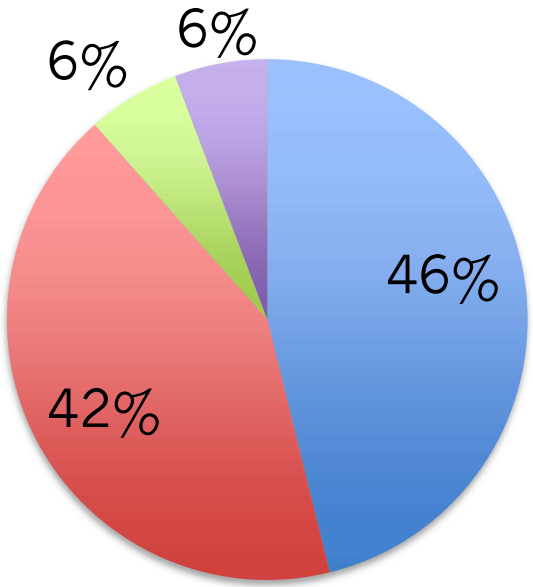
アンケートは「設問への投票」と「自由記入コメント」に加え、「自由記入コメント」に対する「賛同票」と「反対票」の投票を受け付け、アンケート回答者の生の意見を吸い上げる取り組みを行った。

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。

なお、質問の項目により回答数にばらつきがあるのは、WEBアンケートの時間制限から回答時間を締め切ったことが影響している。

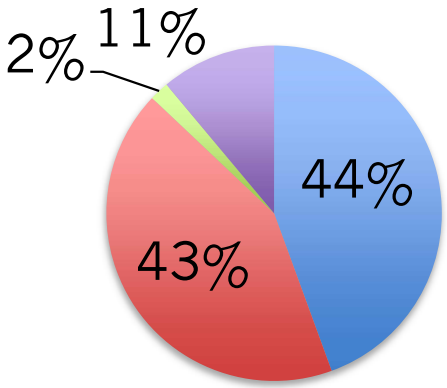
アンケートにご協力いただいた皆様に御礼を申し上げます。

2.1. ご自身の所属組織を選んでください

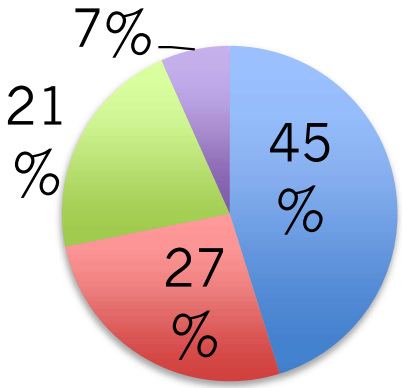


- 民間企業（24）
- 行政機関（22）
- 大学・研究機関（3）
- その他（3）

コミュニティ2018参加者

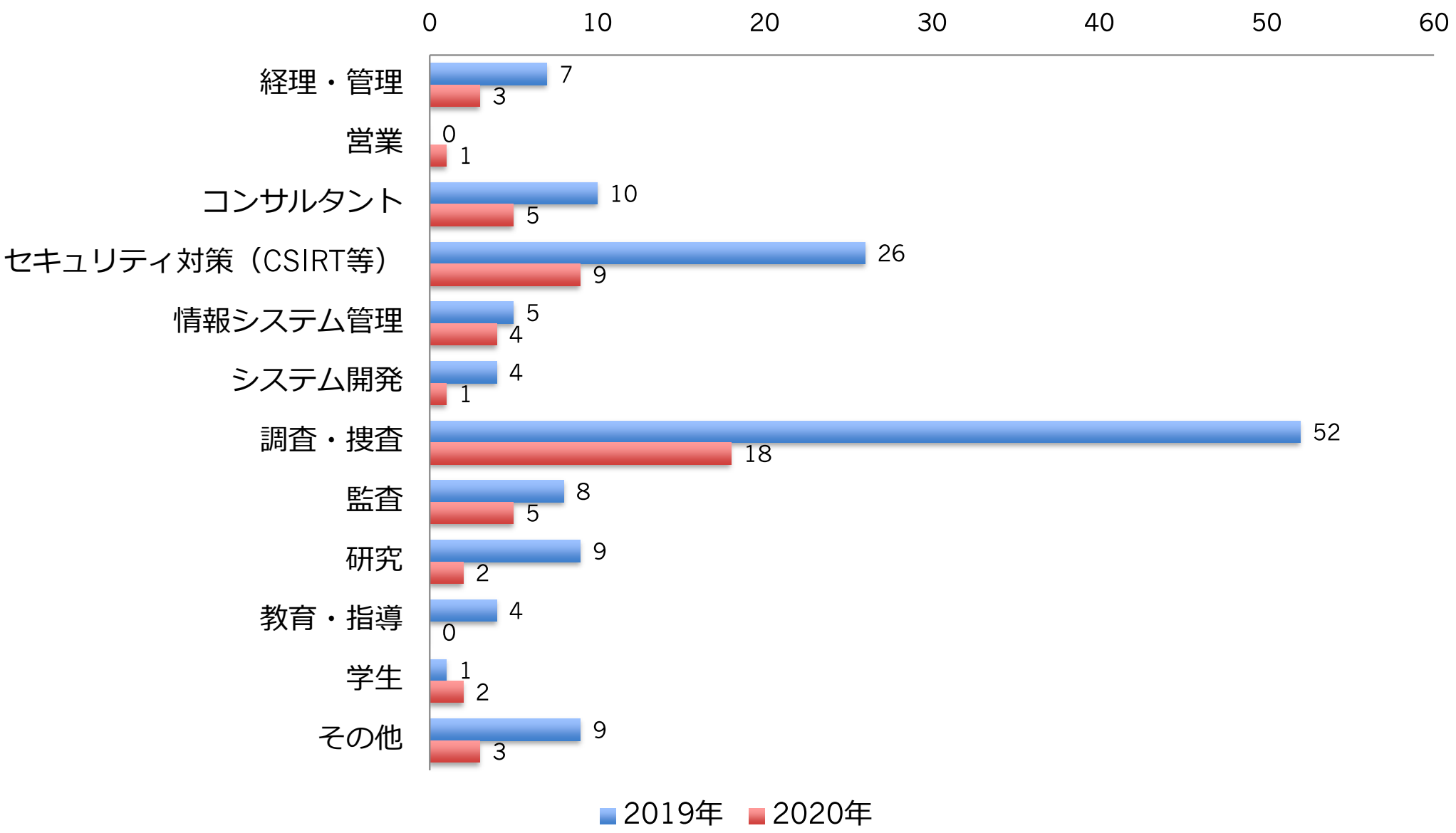


コミュニティ2019参加者



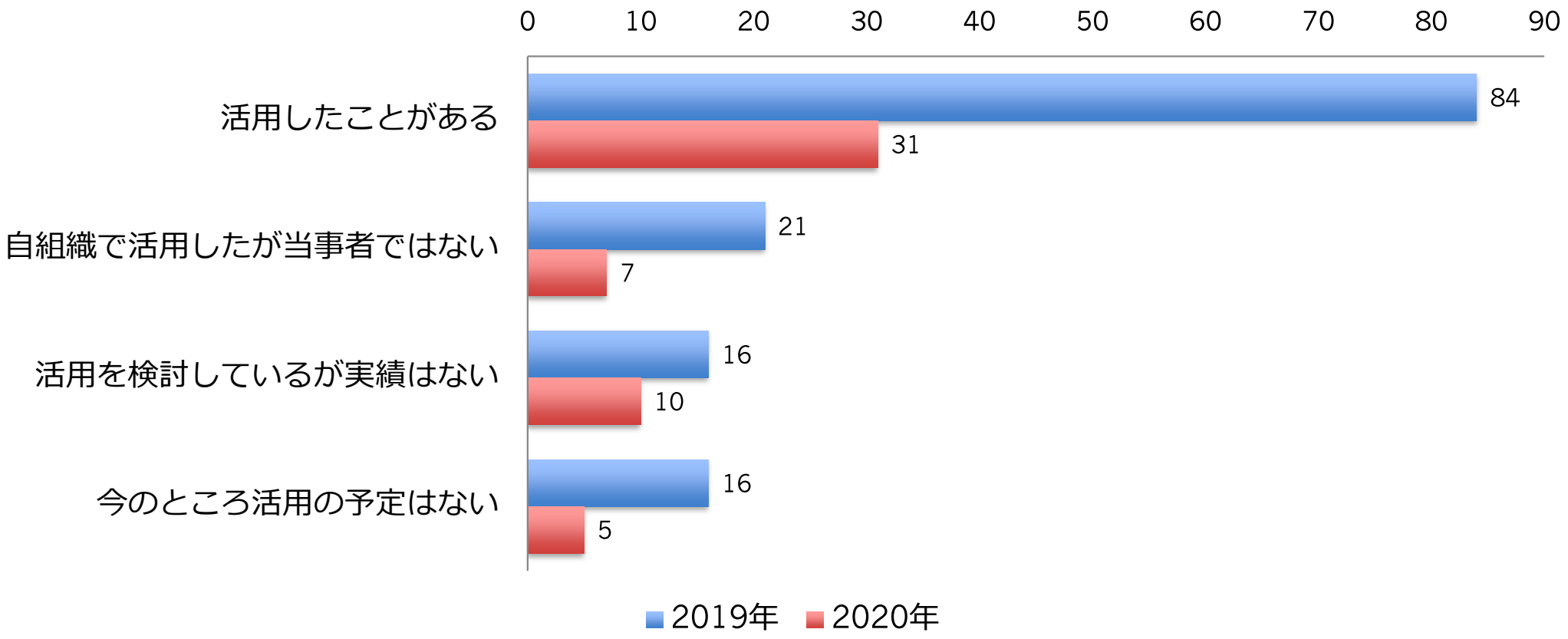
2.2. ご自身の現在のお仕事を選んでください

（１つだけ選択）



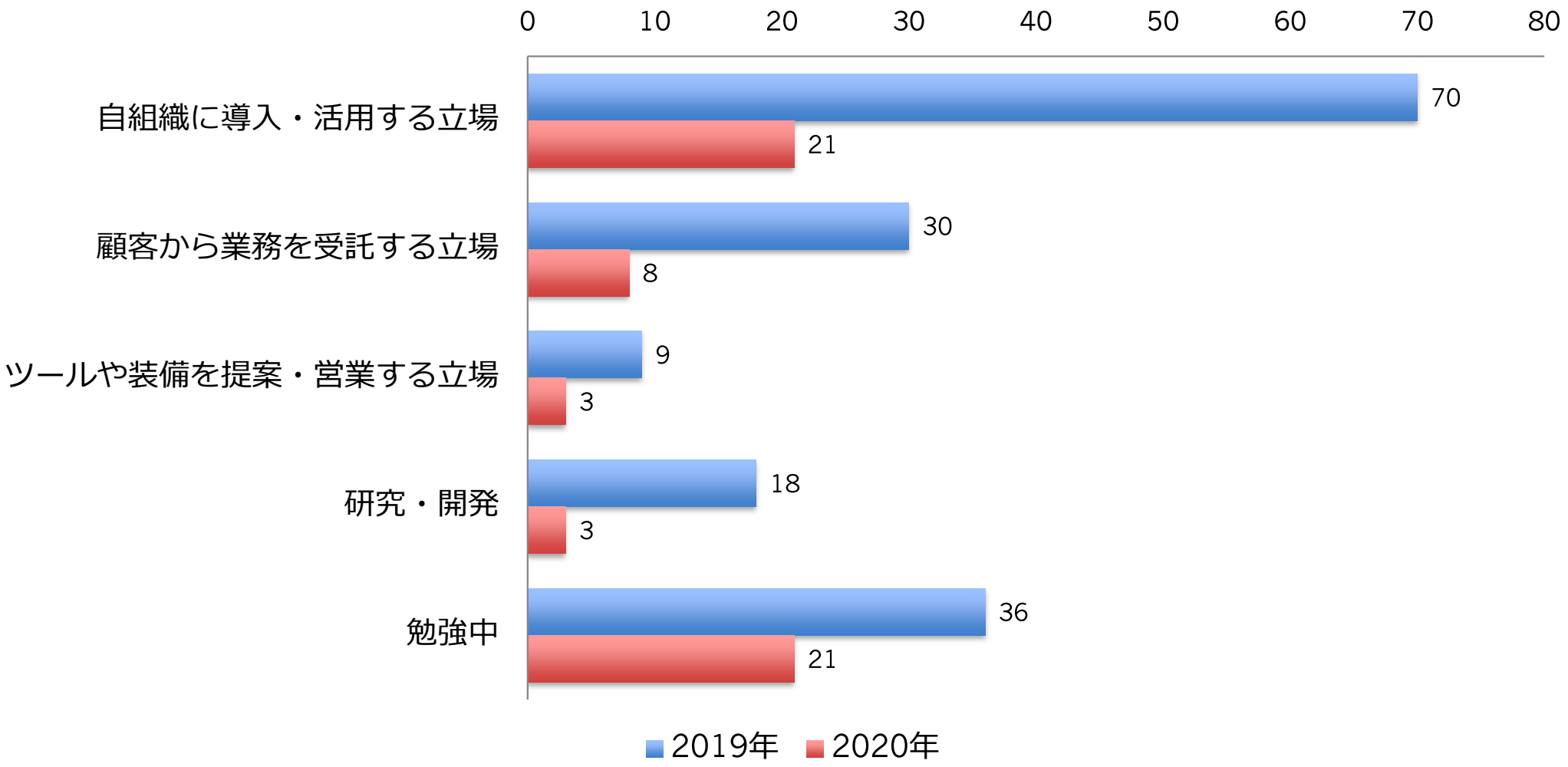
2.3.デジタル・フォレンジックの活用経験は？

（１つだけ選択）



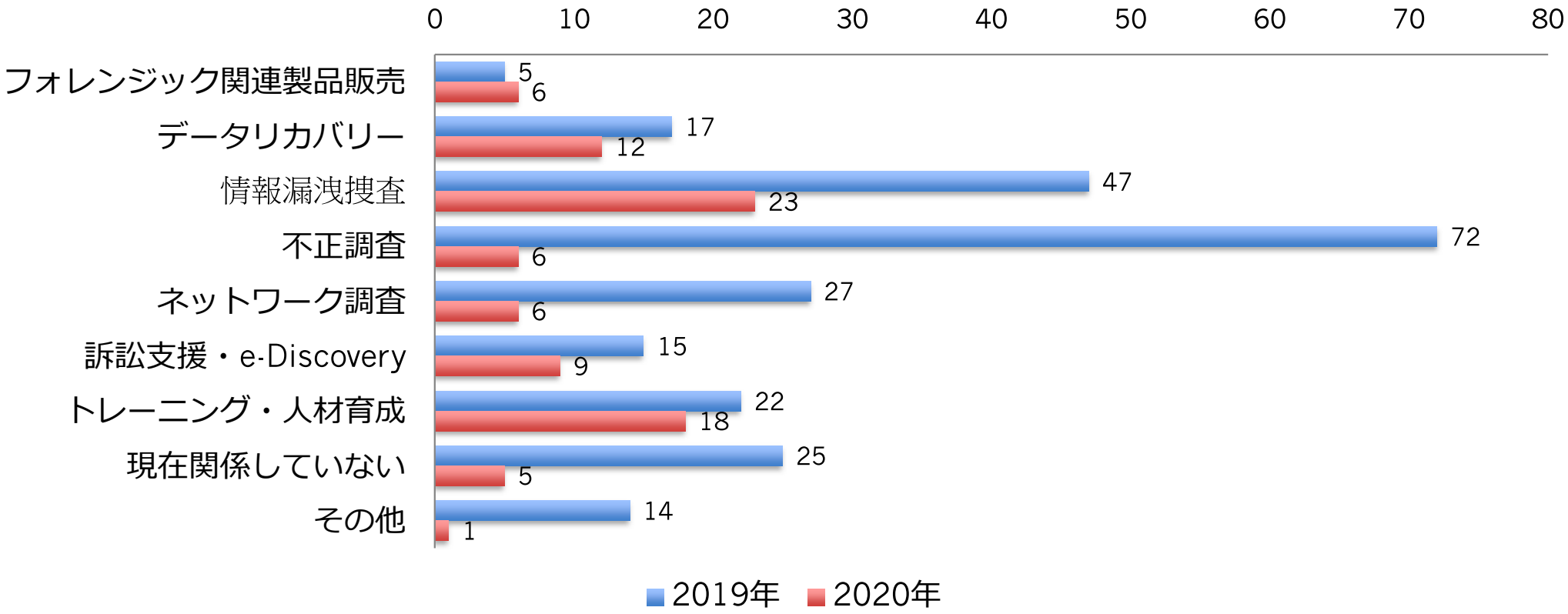
2.4. ご自身が「デジタル・フォレンジック」に関わる立場を教えてください

（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）



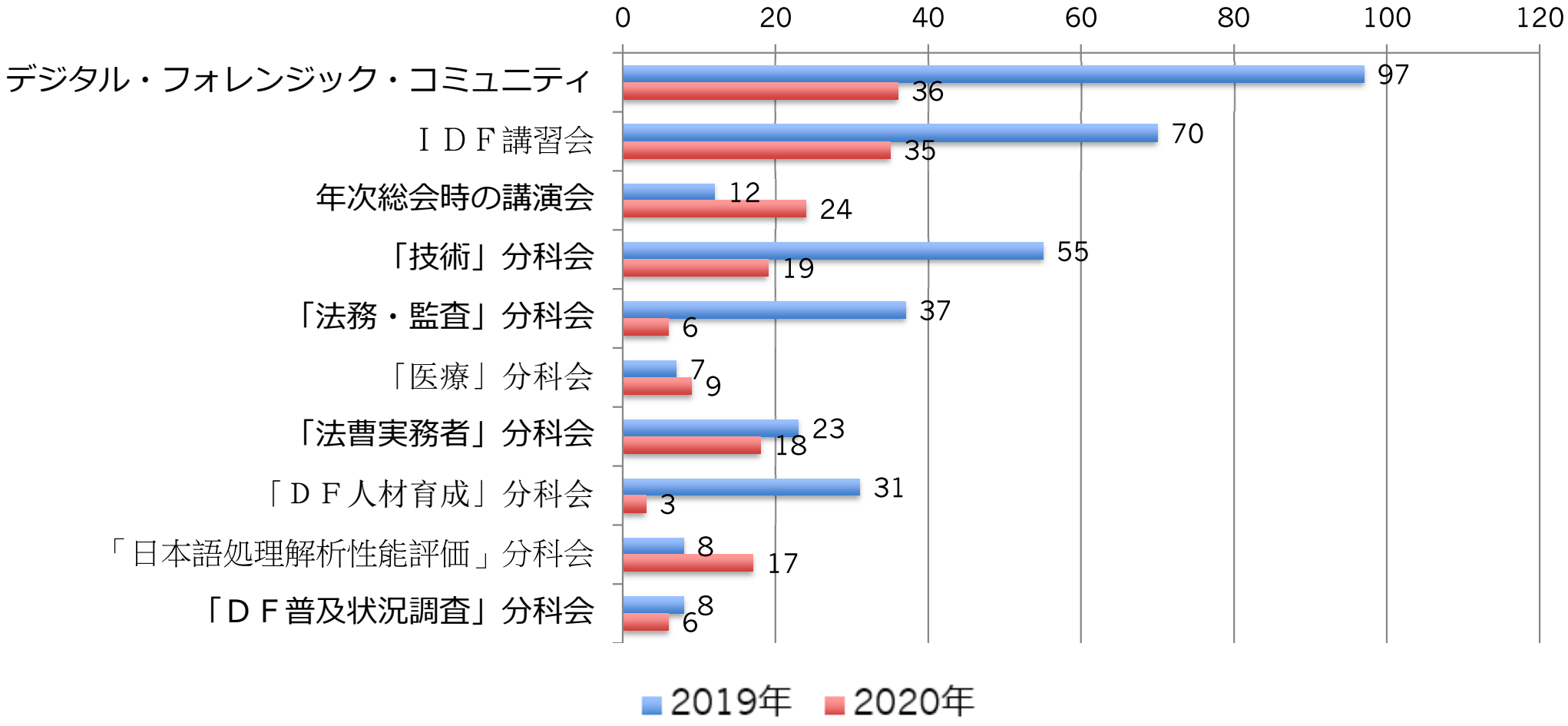
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【 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

【 2020年】
- 犯罪捜査

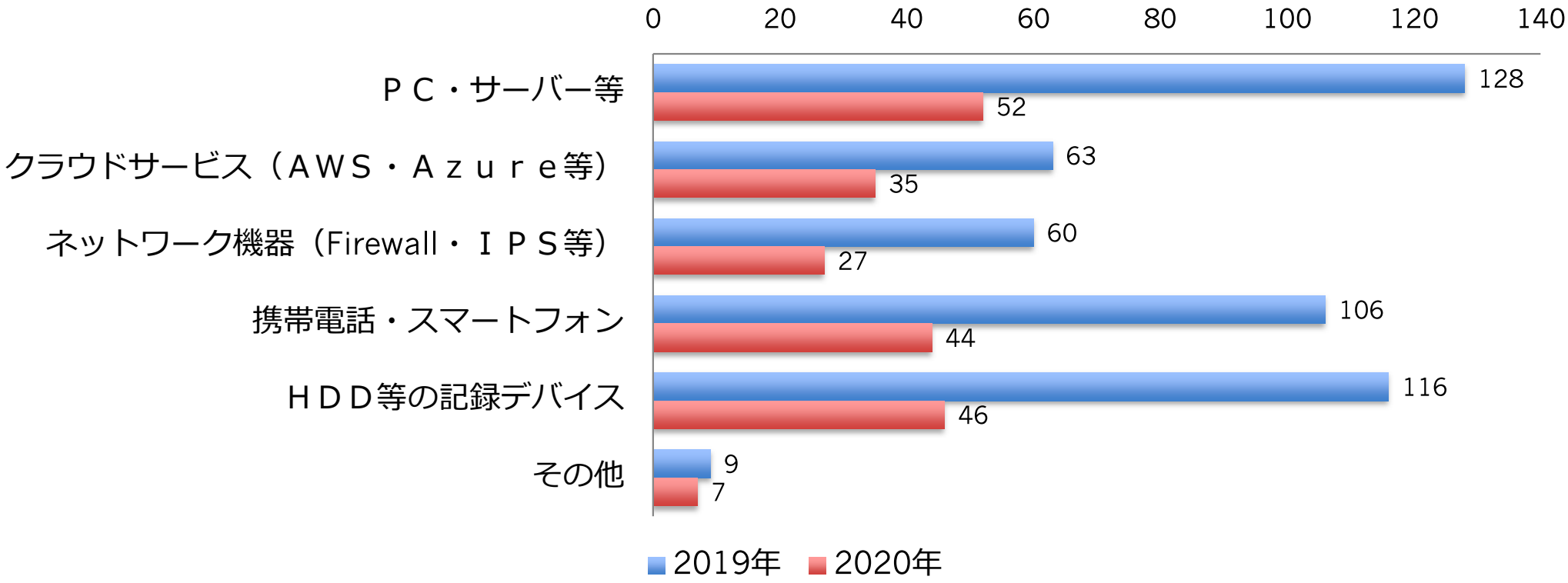
2.6. デジタル・フォレンジック研究会の活動で参加してみたいものは？

（複数回答可）



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）



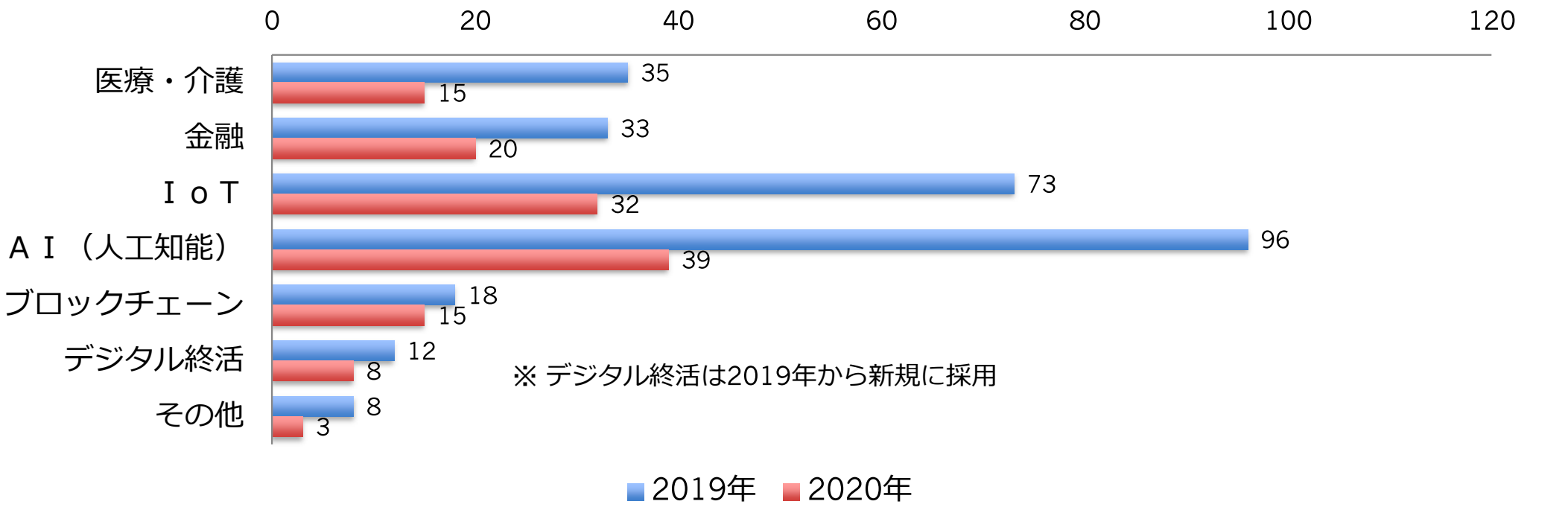
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

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

【2020年】
- IoT機器　+7

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）



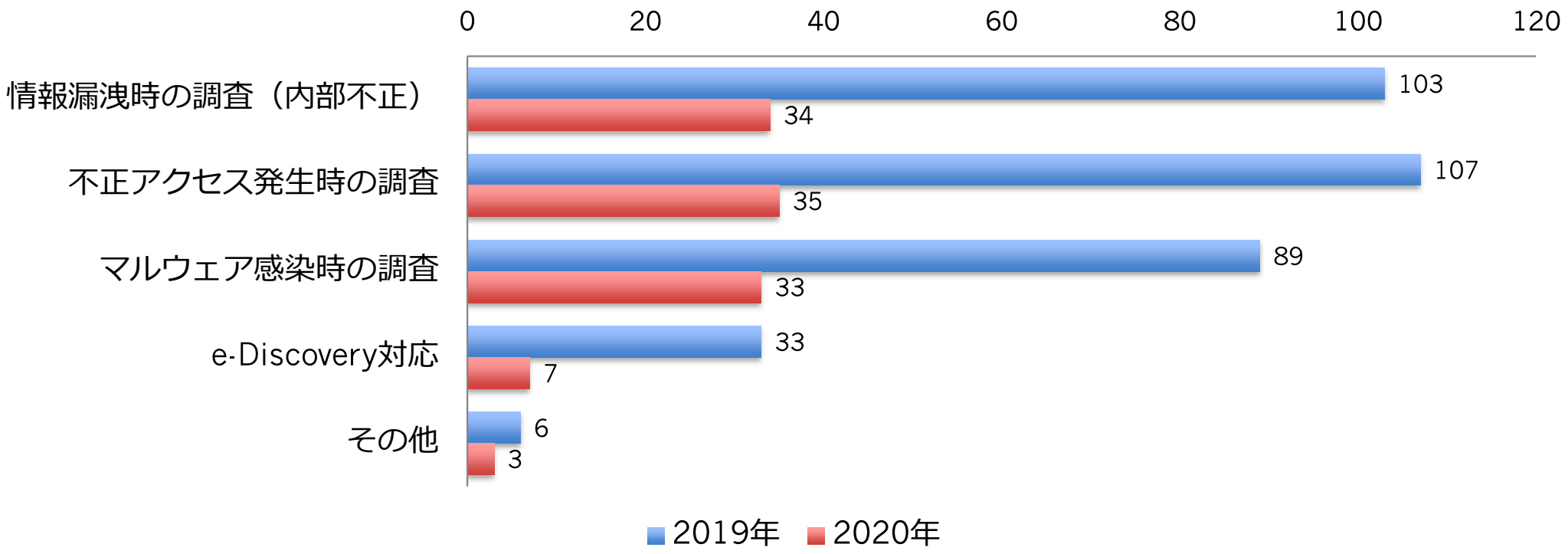
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【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

【2020年】
- 不動産

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）



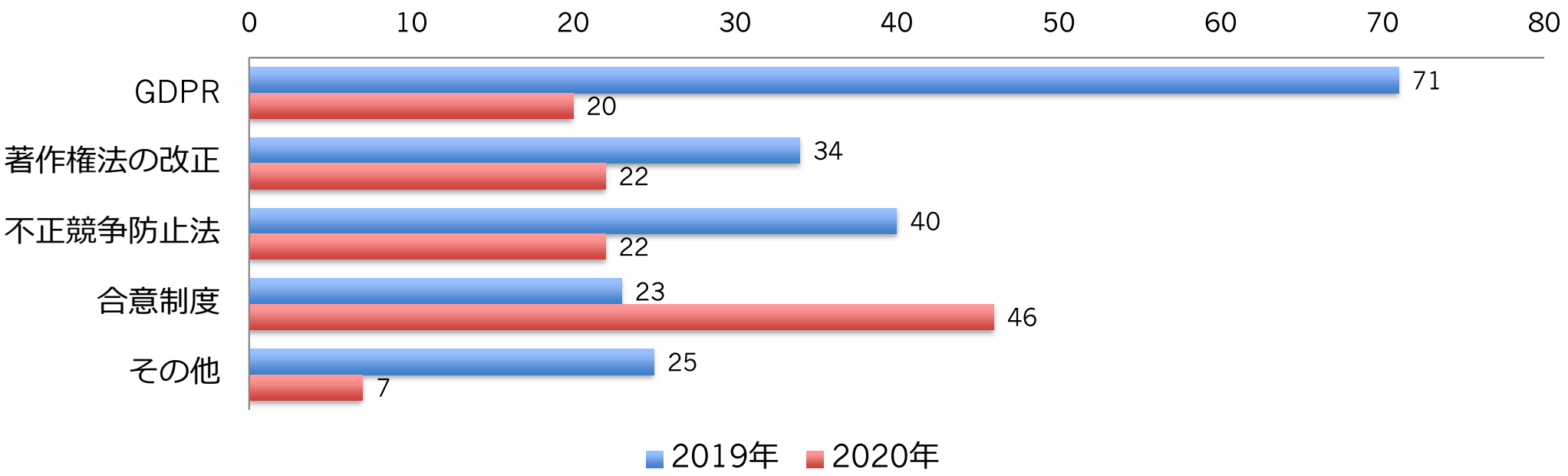
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【2019年】
- パワハラ・セクハラ調査　+7
- 犯罪捜査

【2020年】
・自由記入は無かった

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）

【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

【2020年】

- インサイダー取り引き

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	22	16.FTK Imager Lite, FTK Imager	23
2.analyzeMFT	3	17.Ghidra (NSA)	3
3.Arsenal Image Mounter	4	18.Griffeye	0
4.AXIOM / IEF [Internet Evidence Finder] (Magnet Forensics)	11	19.HX-Recovery for DVR & NVR	0
5.Belkasoft Evidence Center (Belkasoft)	3	20.IDA Pro (Hex-Rays)	5
6.BlackLight / MacQuisition (BlackBag)	8	21.Intella	3
7.Cain	4	22.Kali Linux	21
8.CDIR Collector (Cyber Defense Institute Incident Response Collector)	8	23.Kansa	0
9.DEFT(Digital Evidence&Forensics Toolkit)DART(Digital Advanced Response Toolkit)	8	24.KAPE (Kroll Artifact Parser and Extractor)	0
10. Email Auditor 19(メール監査ツール)	0	25.KIBIT Automator(AIツール)	0
11.Eric Zimmerman ツール	1	26. LACE	0
12.Event Log Explorer	4	27.Lit i View E-DISCOVERY(データ解析ツール)	0
13.Final Forensic / AndrEx (AOS)	10	28. Lit i View XAMINER(データ解析ツール)	3
14.F-Response	1	29. Log Parser(Lizard)	1
15.FTK [Forensic Tool Kit] (AccessData)	19	30. MacQuisition	9

※製品概要は別紙参照

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
31. Magnet RAM Capture	1	46. Redline	0
32. Magnet Acquire	0	47. Rekall	1
33. MSAB Office	2	48. Responder Pro	1
34. Net Hunter	3	49. SIFT Workstation（SANS）	3
35. Nuix Workstation	0	50. Simple SEIZURE TOOL for Forensic（SSTF）/for Android（SSTA）	5
36. Nuix Investigate	4	51. Splunk	7
37. Nuix Discover	3	52. Tsurugi（剣）Linux	5
38. Oxygen Forensic Detective	11	53. TZWorks（の各種パーサー）	0
39. PassWare Kit	1	54. UFED 4PC（Cellebrite）	16
40. PC-3000	6	55. UFED Mobilogy Touch	3
41. Phone Breaker（Elcomsoft）	2	56. VFC5（Virtual Forensic Computing）	3
42. Paladin Linux / RECON(SUMURI)	0	57. Volatility Framework	3
43. Plaso	1	58. VizX（Ziuz）	2
44. RECON IMAGER	0	59. X-Ways Forensics	16
45. RECON LAB	0	参加者から自由記入：Encase	1

※製品概要は別紙参照

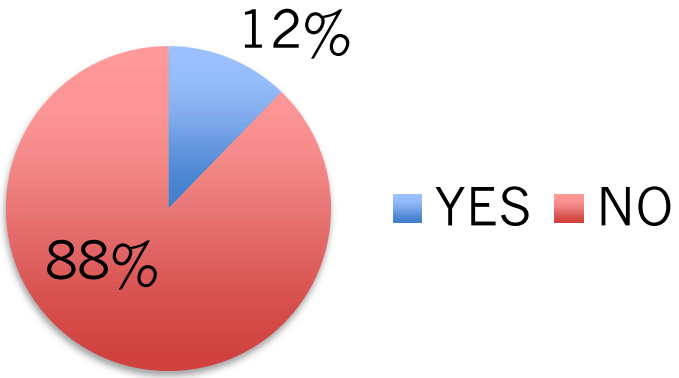
●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

【2020年】
- Encase*　+6

*Encaseは取り扱いベンダから登録申請がなく、2020年の調査対象から漏れていたことが後から判明した

2.12.フォレンジック作業をリモートワークで行っていますか？

「事前準備・打合、データ分析、データ保全」など、リモートワークで行っている作業をお答えください



●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）

- 証拠保全　+2
- フォレンジック対象物の受け渡し
- ツール等の評価、規格化
- クラウド
- VDI
- データの持ち出し
- BYODの個人端末をどう扱うか
- データの漏洩
- ヒアリング
- 打ち合わせ議事録画
- 自宅PCのセキュリティ対策
- ゼロトラストの原理原則に基づき、通信暗号化などインフラ整備か必要ではないでしょうか。
- 情報漏洩対策
- ツールの操作が複雑
- リモート保全
- 導入の価格
- 現物の確認
- リモートワークでの保全作業が困難であること。ex. ＰＣ内のHDDやSSDを他の媒体に複製するには専用機器を使用するので現場作業である必要あり。
- 共通的な理解がなく、作業が進まない、期待ギャップが生じるなどの課題が浮き彫りとなった。
- 在宅でのフォレンジック調査は事実上不可能なこと。
- BYOD端末のフォレンジック調査(BYOD端末（私物）を解析者の自宅（リモートワーク先）へ受け渡す方法など)

2.13. 「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）

●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）

- 国際捜査の法制度
- データやノウハウの共有基盤
- データの保存、抽出方法の標準化
- ファストフォレンジック
- DFの事例の共有
- データ検索
- 裁判所でのDF証拠の標準化
- クラウドデータの解析、証拠保全の標準化
- 金融、国防
- 多要素認証
- 証拠保全（ネットワーク）など
- Apple社のデジタルフォレンジック業務への協力
- ツールの一元化
- 実務でのDF普及
- 国防・安全保障
- 情報漏洩
- 情報収集及び解析のAI利用によるさらなる自動化。
- 拡がっていくと考えます
- 予防、早期発見分野へのシフト
- ファスト・フォレンジックの方法論の確立

- 不正アクセス、ハッキング、情報漏洩およびそれに伴う現金要求など増加傾向にあると思います。このような犯罪行為とも思える事柄を未然に防止することが重要と思います。

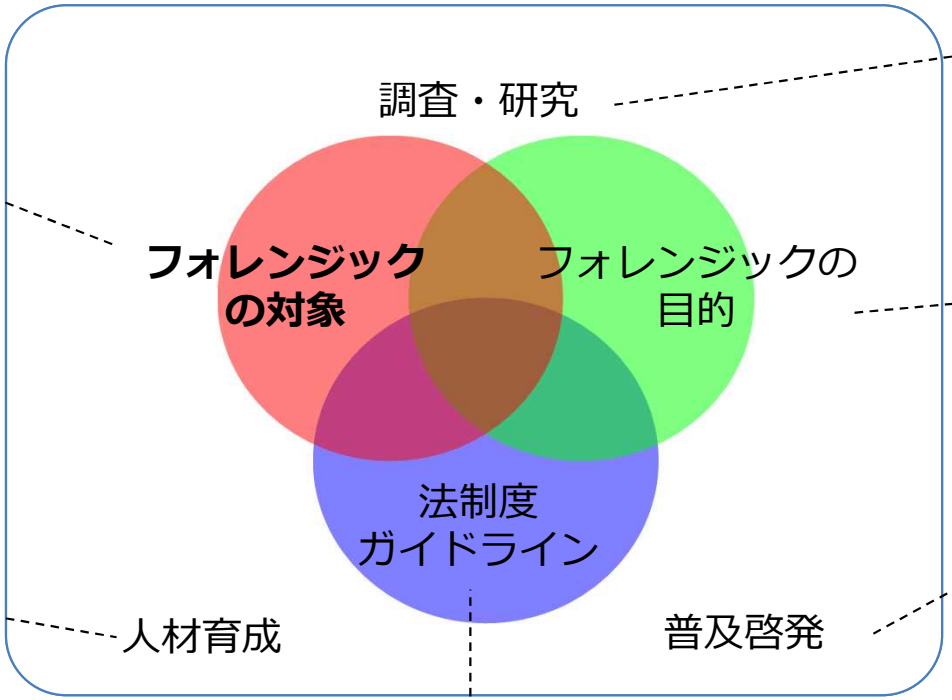
- リモートワークで使われている個々のデバイスの利用状況の概況把握と情報活用。既に製品もあり、活用事例もないことはないですが、製品の導入ハードルが高く、活用事例も極端な内容に思えます。一般的な業務管理の側面からもう少しソフトな導入を行い、通常はあくまで概況レベルの把握にとどめ、必要に応じてディープな内容が精査できる、というやり方ができないものかと思っています。

- デジタル・フォレンジックに期待する分野・方向性としては海外のクラウドサービスなどの越境捜索問題（国際的な議論等）

参考：2019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）

●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

参考：2019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　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

参考：2019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　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

3. 考察と今後の取り組み

1. 調査手法について

- 本アンケートはオンラインアンケートシステムを活用して、コミュニティ会場の参加者とインタラクティブに、またリアルタイムに投稿内容を共有することで、参加モチベーションを高め、多くの回答数と多彩な意見を引き出してきた。
- しかし今回はコロナ禍で、コミュニティ会場への来場者が少ない状況で、リモートからのアンケート参加者も限られており、昨年度(137名)と比較すると半数以下の62名に留り、自由記入等の回答数も大きく減少した。
- 2021年度のアンケート実施時期は、引き続きデジタルフォレンジックコミュニティに合わせて行うこととしたいが、調査方法はＤＦ普及状況調査ＷＧで検討し、見直しをかけていくこととしたい

2. 回答内容の分析について

- 2020年の回答内容は2019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。
- 一方で、デジタルフォレンジック関連業務をリモートワークで実施できていると回答した割合は12%であり、顧客環境からのデータの持ち出しなどが課題となっている様子が伺える。コロナ禍が継続するようであれば、リモートワークにおける工夫など、関係者の課題の共有につながる調査項目を検討していきたい。

3. 今後の取り組み

- デジタル・フォレンジックコミュニティの壇上で行うWebアンケートは、毎年の恒例行事となっているが、ややマンネリ化しており新たな進化が求められている。
- 今後の取り組みとしては、デジタル・フォレンジック研究会関係者の業務に資する調査項目を充実させるなど、アンケート調査手法を含めてＤＦ普及状況調査ＷＧで検討していく。