2017年度
デジタル・フォレンジック
普及状況調査 報告書

2018年3月31日
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

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う。

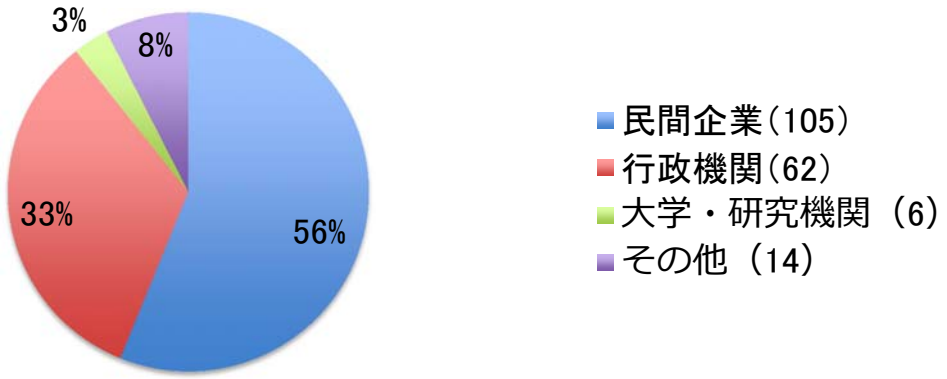
2017年度の調査では、昨年度の調査手法等の課題を踏まえ、セミナープログラムに「20分間のWEBアンケート」を設けて、述べ187名の参加者からオンラインのWEBアンケート等の調査にご協力をいただいた。

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」の投票を受け付けた。

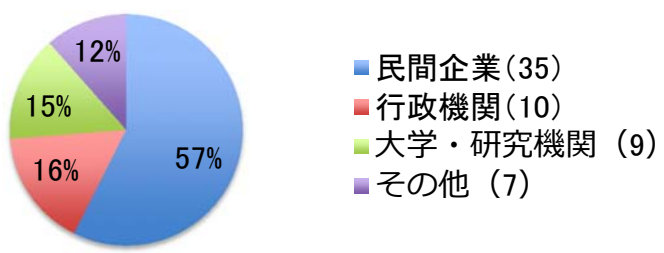
調査結果については、WEBアンケートと紙アンケートの両方に回答した参加者の峻別が困難なため単純に合算した結果をまとめている。

- WEBアンケート集計結果‥‥‥‥　100件
- 紙アンケート集計結果　‥‥‥‥　87件

2.1. ご自身の所属組織は？

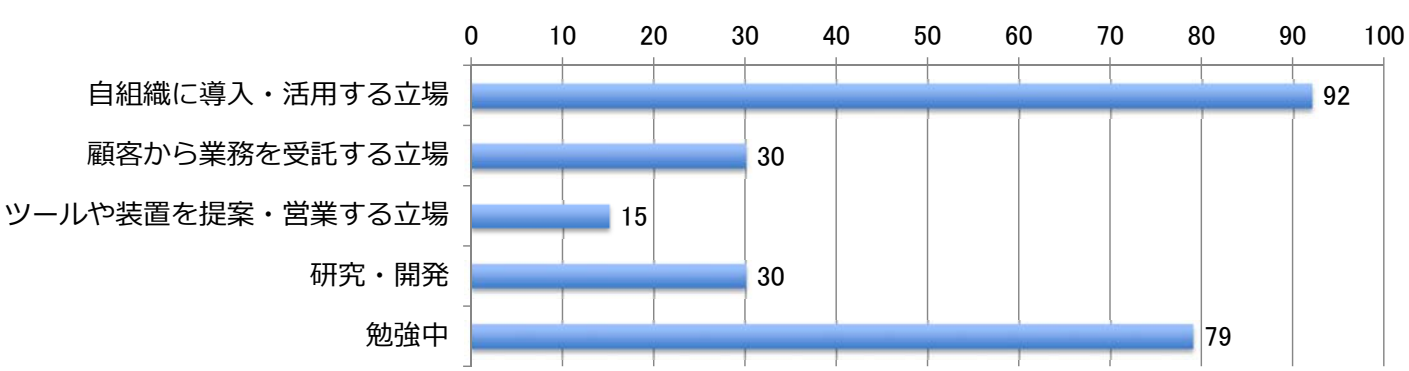


参考：デジタル・フォレンジック・コミュニティ2016の交流会参加者の所属組織



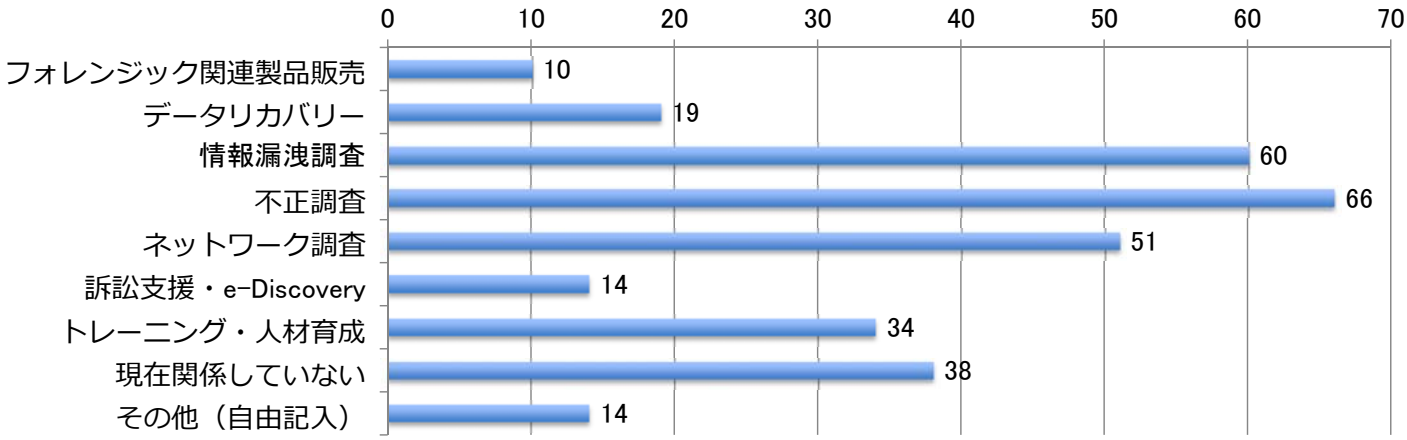
2.2. ご自身が「デジタル・フォレンジック」に関わる立場を教えてください

（複数回答可）



2.3. 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）

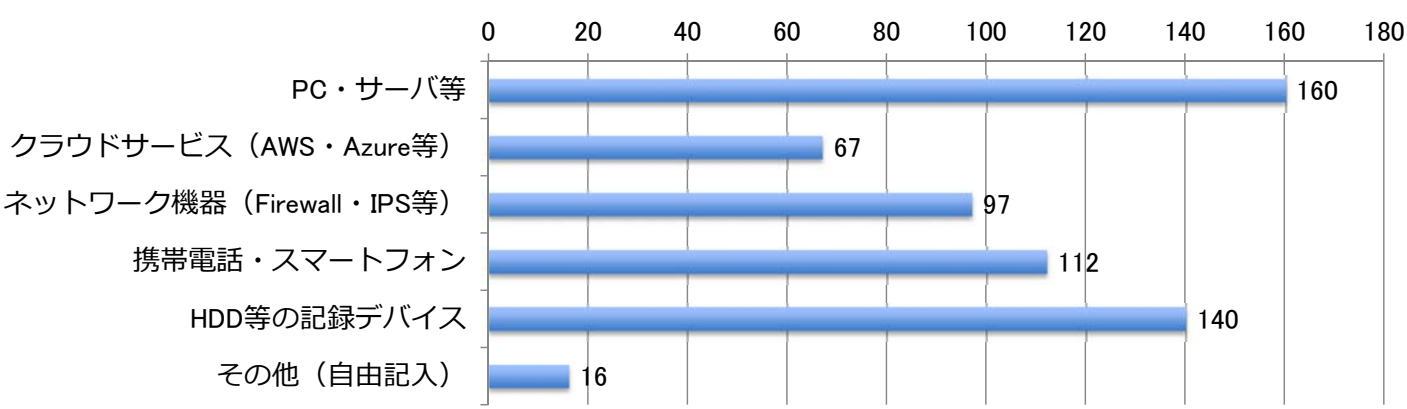


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（－）

- マルウェア解析　＋2
- 犯罪捜査　＋1
- 捜査におけるデジタルフォレンジック
- スマートフォン解析
- 担当内で該当業務を実施している
- メディアとしての情報配信

2.4. 「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）

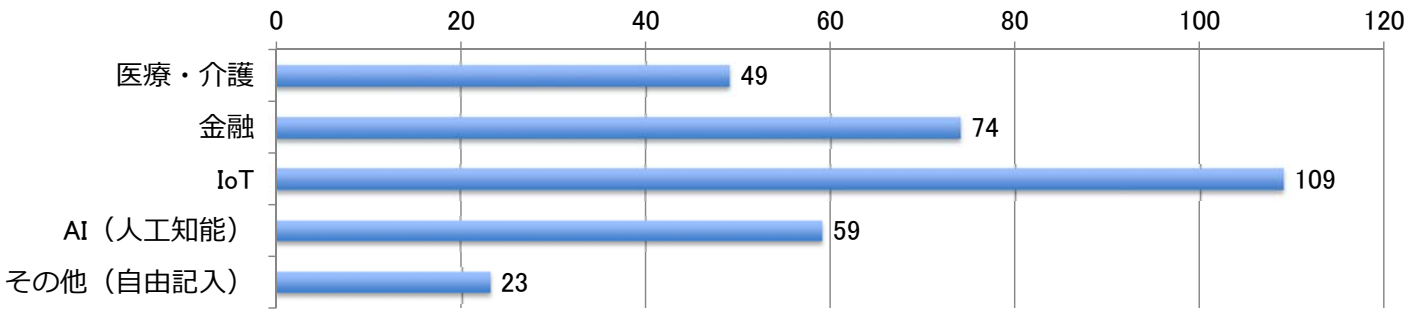


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（－）

- IoT　+22
- デジカメ　+14
- カーナビゲーション　+11
- メモリ　+5
- よく分かっていない
- 悪意ある攻撃者が有する電子機器
- GPS
- ネットワークトラフィック

2.5. 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）

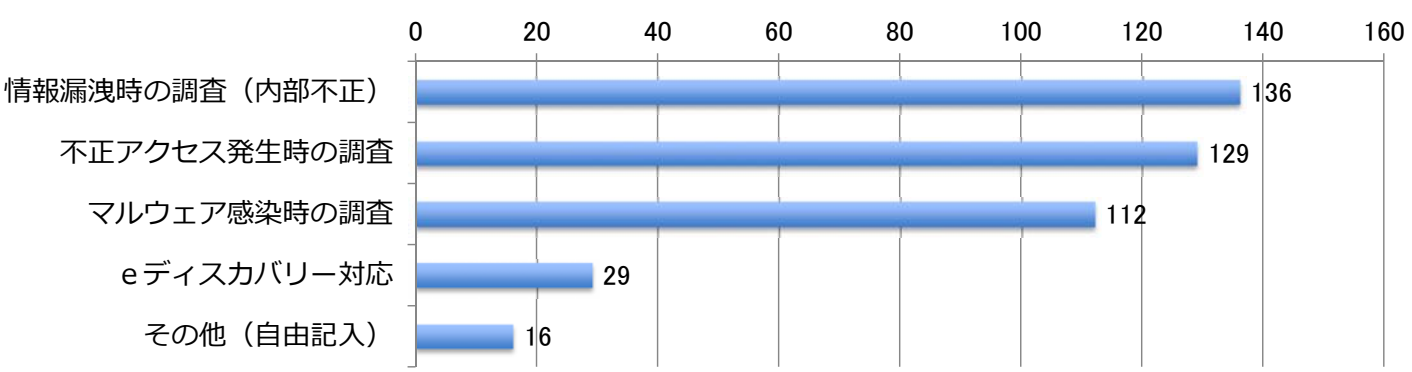


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

- ドローン　+3
- ビッグデータ解析　+3
- 情報通信業との連携　+4
- 防衛　+9
- 内部不正抑止　+9
- インシデント対応　+18
- 人材採用　+5
- 制御・ライン　+7,-1
- 製造業　+5,-2
- 事故調査　+14,-1
- 移動履歴　+5,-1
- 対応が遅れている産業　+5

2.6. 「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）

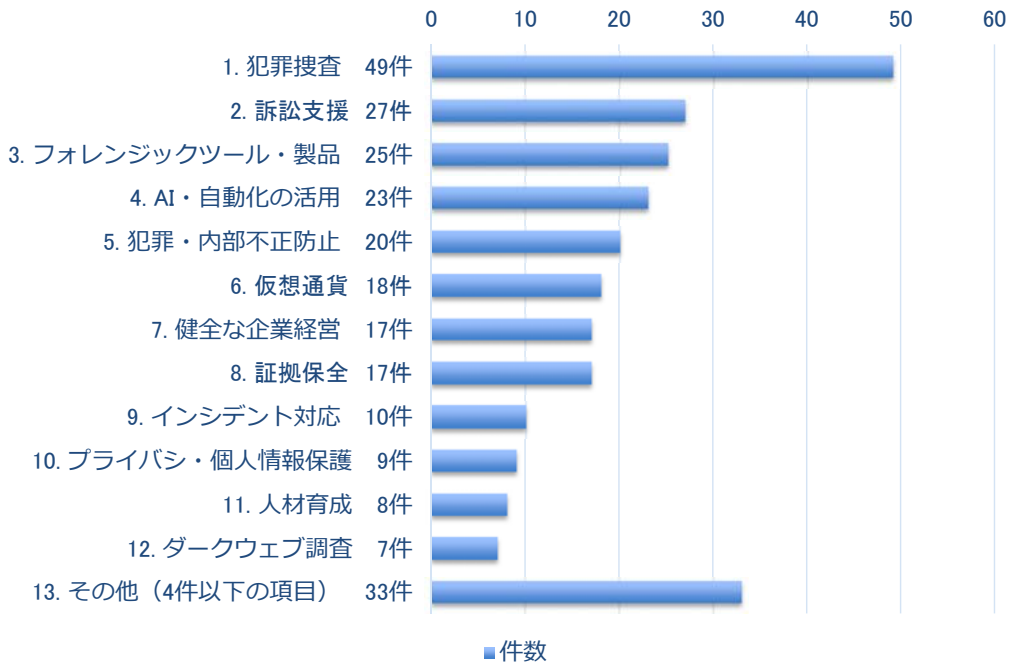


●自由記入コメント：アンケート協力者が入力した文字をそのまま転載、賛同票（＋）反対票（ー）

- 企業の健全化
- AIの暴走阻止　+3
- 自然災害被害回復　+2
- 保険業　+7
- 訴訟支援　+17
- 犯罪調査　+24
- 働き方改革　+6,-3
- 各種犯罪の証拠及び取調べに資する情報の保全
- 証拠保全
- フォレンジック担保の為に使用するデータの復元技術の通常的な分野への展開（情報のレストア）
- DATA RECOVERY, AUDIT

2.7.1. 「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）

●下記の棒グラフは自由記入ア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」と「反対票」を加算したものである。
類似のコメントが4件以下のコメント（15項目）はその他に分類した。



2.7.2. 「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.犯罪捜査 49件
・犯罪捜査＋48

2.訴訟支援 27件
・解析のスピードを上げたい +9
・民事訴訟のIT化 +9
・訴訟支援 +6

3.フォレンジックツール・製品 25件
・製品への当初から導入しておく +8
・高いツールを入れなくても手軽にできるようなツール、システムが充実するとありがたい +6
・無料ツール +4
・利用されているツール +2
・ウィルス対策ソフトへの組み込み

4.AI・自動化の活用 23件
・AI、クラウドを用いた犯罪調査 +7
・AIによる補助 +4
・自動化・簡略化・一般化 +4
・自動化による大規模対応の効率化 +1
・ＡＩによる犯罪抑止、反社会勢力への攻撃
・人工知能を利用したデジタル・フォレンジック
・ＡＩによる自動化

5.犯罪抑止・内部不正防止 20件
・内部不正の防止と働き方改革 +11
・犯罪抑止 +7

6.仮想通貨 18件
・仮想通貨 +6
・Fintechやブロックチェーンとの関連 +6
・送金決済 +3

7.健全な企業経営 17件
・クリアな企業運営 +7
・企業の説明責任 +4
・有価証券報告書での開示 +3

8.証拠保全 17件
・IoT機器の証拠保全 +14
・データ保全（大容量データに対するアプローチ）
・削除データの復元、証拠保全

9.インシデント対応 10件
・インシデント発生への備え +6
・秘匿化した社名で今まで非公開だった脆弱性を公開・集約・共有してほしい +2

10.プライバシー・個人情報保護 9件
・プライバシー保護 +7
・個人情報保護に関するもの

11.人材育成 8件
・フォレンジック技術を学べる場 +6
・捜査機関の人材育成に向けた情報・知見共有

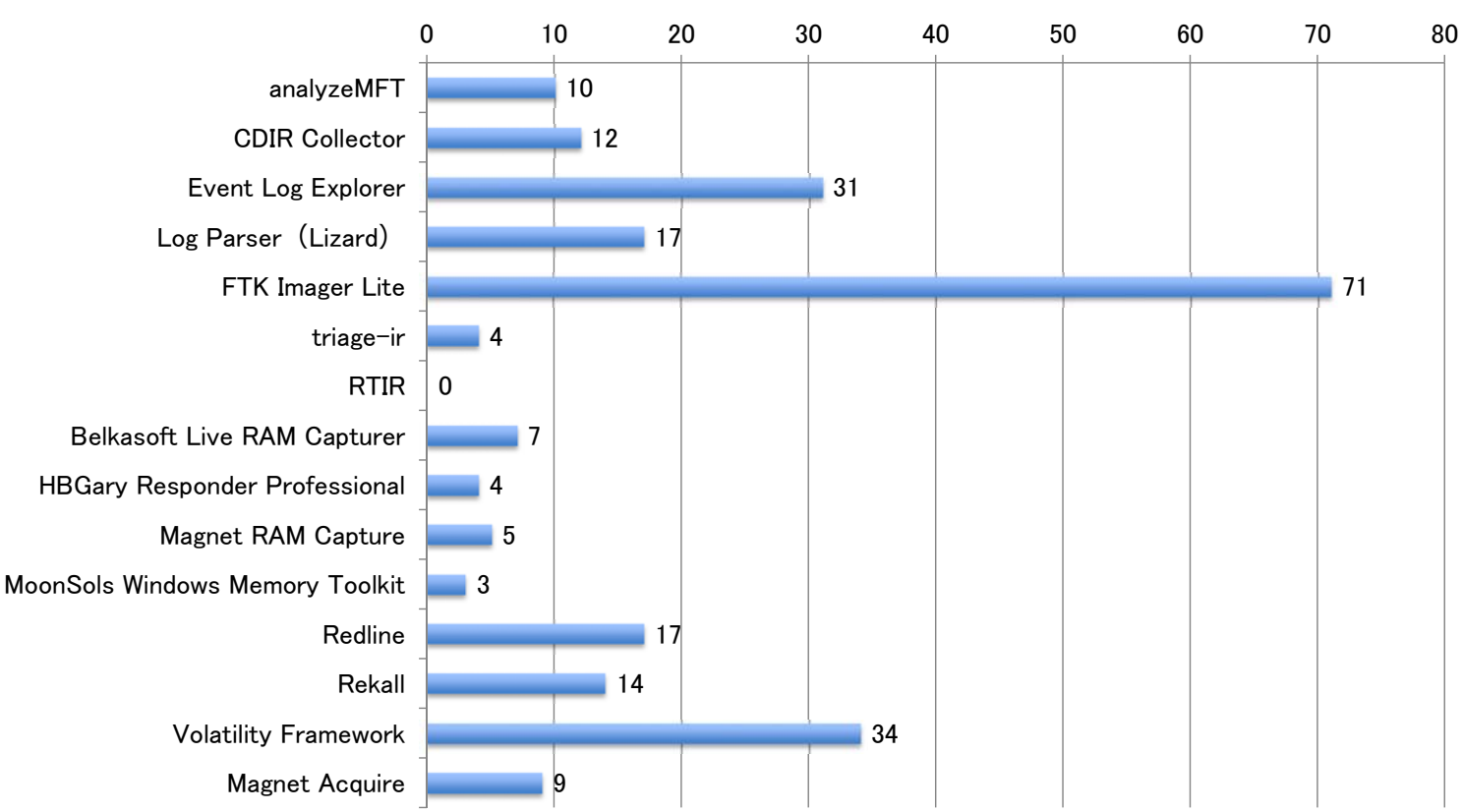
12.ダークウェブ調査 7件
・ダークウェブ調査 +6

2.7.3. 「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）

13.その他、今後への期待等　33件
・他国の状況　+3
・知的財産　+3
・森友　+3
・長期フォレンジックデータの価値とコストのバランス　+2
・アンチフォレンジックの方向性について　+2
・総SSL通信化におけるネットワークフォレンジック　+1
・人格分析　+1
・グローバルな調査では法律がネックになる。これが障壁とならない調査方法を持ちたい　+1
・情報通信業と連携し、フォレンジックが活用できるフィールドでの活動を円滑にすることを期待する　+1,-1
・デジタル・フォレンジック端末が万人に扱えるほどの単純捜査になっていく
・フォレンジック情報の価値とデータ量、コストのバランスについて（特にネットワークフォレンジックにおけるRawデータの扱いにおいて）
・セキュリティが強化されるモバイルデバイス（スマホ等）の適正な証拠収集方法、保全処置
・広範な分野での活用
・希望退職者や鬱病社員の早期発見
・クラウド分野

2.8. 使ったことのあるツールを教えてください（複数回答可）



3. 考察と今後の取り組み

1. 調査手法について
   - 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にて調査を行った。
   - 2016年度はネットワークトラブルに見舞われたが、2017年度はトラブルのバックアップ環境を用意し、円滑な運営が可能となった。

2. 調査した環境について
   - 2016年度は交流会会場（立食パーティ）で実施した。2017年度はコミュニティのプログラムとして着席状態15分間のオンラインアンケートシステムで実施し、多くの回答を得たことから2018年度以降も同様の取り組みを行うこととしたい。

3. 回答内容の分析について
   - 2017年度のアンケート項目は2016年度の試行実施結果を踏まえて変更しており、単純に経年変化の比較をできるものにはなっていない。しかし、2年間を通じて回答を得ているデジタル・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）や今後有望な分野（IoT）への回答は一致しており、アンケートの参加者層や意識は概ね似た状況にあると思われる。
   - 2018年度は2017年度のアンケート項目と同じ項目を再度取得することを基本に取り組み、深掘り分析を行うこととしたい。
   - 2018年度に起きた特徴的なインシデントについては、適宜WGメンバの意見を取り入れアンケートに盛り込み、デジタル・フォレンジックの最新動向調査と情報共有に役立てることとしたい。

4. 今後の取り組み
   - 2018年度のアンケート調査は、デジタル・フォレンジック・コミュニティ2018のプログラムの枠の中で、アンケート対象者が着席時に15分間程度行うこととしたい。（休憩の後の時間枠が望ましい）
   - 2017年度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、2018年度も自由記入を充実させる工夫を行うこととしたい。
   - 2017年度調査結果の報告会を開催するとともに、調査結果の生データ（CSV）についてもIDFのWEBサイトで公開することとする。