特集
Special Feature

［最新のデジタル・フォレンジック事情］

5 デジタル・フォレンジックの普及状況について
―関係者アンケートから考察するデジタル・フォレンジック―

応 般

小山　覚　NTT コミュニケーションズ（株）情報セキュリティ部／特定非営利活動法人デジタル・フォレンジック研究会

デジタル・フォレンジック（以下，DF）の活用目的

本稿は特定非営利活動法人デジタル・フォレンジック研究会（以下，IDF）の活動の一環として，同研究会のイベント参加者に対して毎年行っているアンケート調査結果をもとに，筆者が推考しとりまとめたものである．多分に私見が含まれている点をご容赦いただきたい．

このアンケート調査は 2016 年から行われている．すべての期間を通じた回答から，DF の対象である記憶媒体は従来のパソコンやスマホから，クラウドや IoT デバイスなどに拡大している．その一方で DF が有益と考えられている活用目的は，ディジタル遺品などに多様化しつつも，毎回の調査で上位は「情報漏洩・不正アクセス・マルウェア感染」時の対応が挙げられており（図 -1），DF のビジネスにおける主戦場はおおむね定まっているようだ．

なお，本稿で紹介するデータは，直近 3 年間のアンケート結果に基づいている．興味を持たれた方は，IDF Web ページ[☆1] から調査報告書をダウンロードしてご覧いただきたい．

DF 普及状況を調査する目的

DF 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，また証拠能力のある情報を得る手段として活用され，犯罪捜査だけでなく企業における情

☆1 https://digitalforensic.jp/

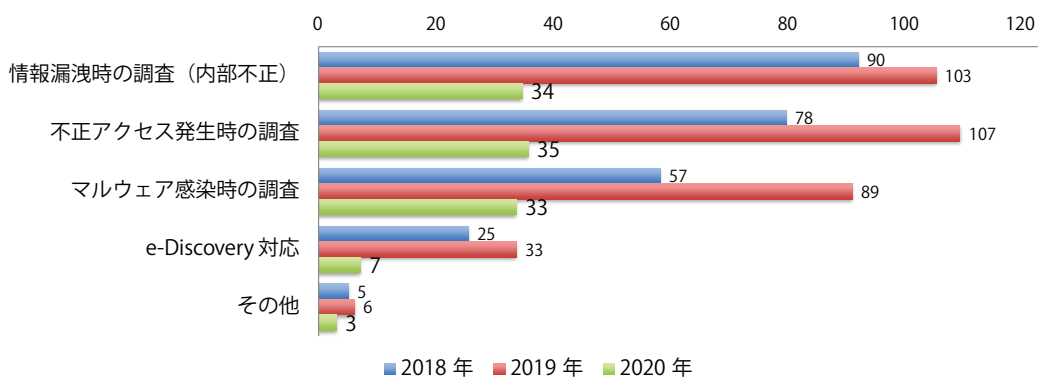

図 -1
DF の有益な活用目的

© 2021 Information Processing Society of Japan

報漏洩インシデント対応においても必須の技術として発展してきた．その一方で，DF は第三者に知られたくない場面で利用されることも多く，その普及状況はセキュリティ製品やサービスのようには知られていない．

そこで，DF 製品やサービスの導入・使用状況や，DF を活用する関係者の意識や，ユーザの期待を調査することで，DF の関係者の参考となるデータをまとめることを目的に DF 普及状況の調査を行っている．

DF 普及状況調査の方法と対象者

DF 普及状況の調査方法

DF 普及状況の調査は IDF のイベントプログラムの一環として実施しており，イベント会場においてセミナー形式で画面投影した Web アンケート内容を解説しつつ，その集計結果をリアルタイムに共有する方法で行っている．また Web アンケートに参加できない人のために事前の紙アンケートも併用し調査結果にまとめている．

DF 普及状況調査の対象者（イベント参加者のプロフィール）

2018 ～ 2020 年に行った 3 回のアンケート対象者は述べ 307 名（2018 年 108 名，2019 年 137 名，2020 年 62 名）で，多い順に「民間企業，行政機関，大学・研究機関」に所属している．また回答者が従事している業務は，多い順に「調査・捜査，セキュリティ対策（CSIRT 等），監査，コンサル」などで，DF を実務で活用する業種や職種が多数を占めている（図 -2）．

DF の活用経験に対する問いに対しては，「半数以上が活用経験あり」と回答している．回答者の DF との関係は多い順に，「自組織に導入・活用する立場，勉強中，顧客から業務を受託する立場」，となっており，DF がすでに企業等の現場で活用されていることがうかがえる．

アンケート結果から DF の現状と未来を読み解く

開花した DF の業務分野

DF 普及状況調査の蓋を開けてみると，DF はすでに多くの分野において，調査や捜査のツールとして定着し，さまざまな関連分野を生み出している状況が確認できた．

3 回の調査において回答者が関係している業務は

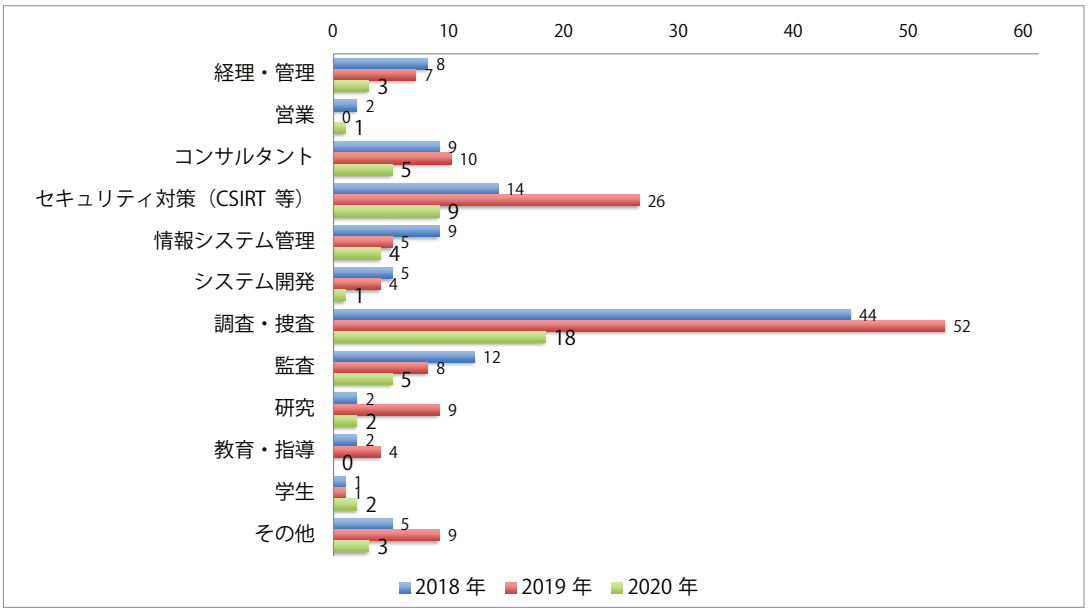

図 -2
回答者の従事している業務

© 2021 Information Processing Society of Japan

多い順に，「不正調査，情報漏洩調査や捜査，犯罪捜査，ネットワーク調査，データリカバリー」であるが，回答者の自由記入により寄せられた業務には，「インシデントレスポンス時のファストフォレンジック，ディジタル遺産，研究テーマとしてのDF」など，多様な業務の裾野が広がっている．

さらにDFの普及を支える関連分野では，多い順にフォレンジック関連製品販売，訴訟支援，e-Discovery[☆2]，トレーニング・人材育成が挙げられており，DFを取り巻くすそ野の広がりが確認できた（図-3）．DFは産業としてのポジションを得たと言っても過言ではないだろう．

DF製品の利用状況について

DFのツールや製品は，対象となる記録媒体やシステムごとに「証拠保全」や「調査・解析」の機能に特化したもの，スマホなどのデバイスに対応したDFの全作業工程を包含した「統合ツール」など，さまざまなものが開発され普及している．製品名と機能については誌面の都合で紹介できないが，IDF Webページで調査報告書とともに公開しているのでご覧いただきたい．

☆2 「e-Discovery」とはアメリカなどのコモン・ロー諸国の訴訟法で採用されている証拠開示制度のこと．日本の裁判とは異なり要求された証拠はすべて提出しなければならない．

DFに影響する国内外の法制度について

DFに影響する国内外の法制度は多い順に，「GDPR，合意制度，不正競争防止法，改正著作権法[☆3]」である．合意制度はいわゆる司法取引制度として新たに導入された制度であり，証拠収集や提出段階でDFが活用される可能性がある．米国におけるe-Discovery制度のようにDFの普及を牽引するがどうかは未知数であるが今後の状況を見守りたい．

DFのプロダクト・ライフサイクル

DFのプロダクト・ライフサイクルについて考えてみたい．製品やサービスが市場に投入されてから，寿命を終え衰退するまでのサイクルを体系づけたプロダクトライフサイクルは，導入期・成長期・成熟期・衰退期で表される．

DFの普及・促進を目的に2004年にIDFが設立されている．いまなお活発にIDFの活動が継続していることから，DFはライフサイクルの導入期は脱して，少なくとも成長期に入っていると思われる．近年におけるサイバー攻撃の激化や不正行為の高度化や，IoTデバイスやクラウドサービスなどの新しい環境に対応するため，DF技術は日々進化を遂げており，将来も有望な産業分野であることは間違いない．

☆3 ビッグデータなどに対応した平成30年（2018年）改正のこと．

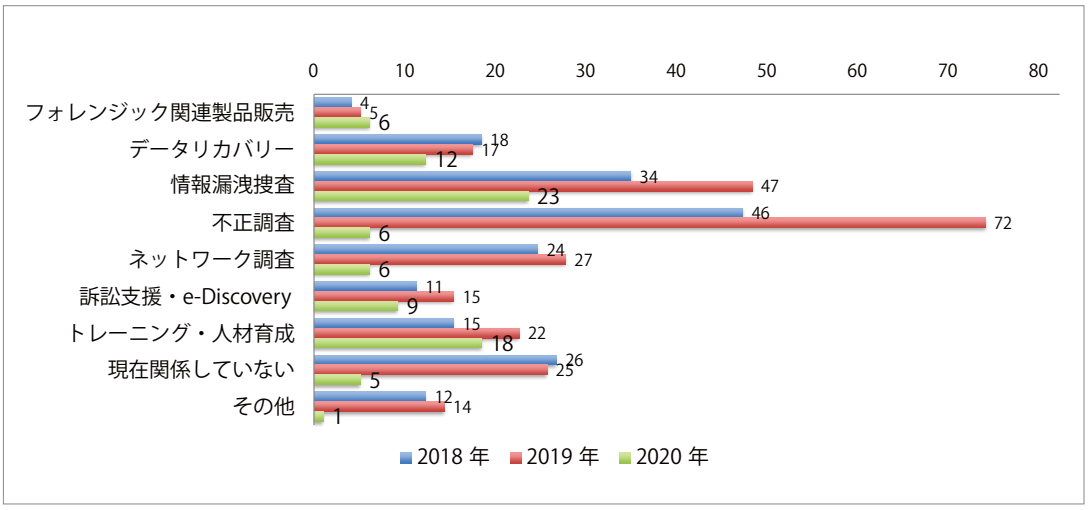

図-3
回答者が関係しているDFの分野

© 2021 Information Processing Society of Japan

本稿の冒頭でも紹介したように，DF と聞いて思い浮かべるものは多い順に，「PC・サーバ等，HDD 等の記録デバイス，携帯電話・スマートフォン，クラウドサービス，ネットワーク機器」などの定番に加え，近年では「IoT デバイス，家電，ドライブレコーダ」などにも DF の対象が広がっており（図 -4），DF が ICT 環境やディジタル環境の変化に追従して成長している様子がうかがえる．

一方で DF が有益な分野は，回答の多い順に「情報漏洩時の調査（内部不正），不正アクセス発生時の調査，マルウェア感染時の調査」が大宗を占めている．2004 年に IDF が創設された当時から DF の三本柱といっても過言でない分野であり，ディジタル遺品などに適用領域が拡大しているが，まだまだ少数派である．DF の産業としてのさらなる成長には，この三本柱以外の新たなビジネス領域の獲得が必要と思われる．

近未来の DF

いま社会生活の大転換期が訪れている．コロナ禍でのリモートワークの定着は言うまでもなく，デジタルトランスフォーメーションによる新たな価値創出が始まり，AI（人工知能）は多くの仕事を人から奪いだした．これまでの DF は人やマルウェアの振舞いをディジタル記憶媒体の解析で明らかにしてきたが，ディジタル化され社会生活の多くを AI に依存する近未来では，AI の振舞いを AI が監視することも増え，その AI の振舞いを DF を使って解析するような，新たなビジネスが生まれているに違いない．

（2021 年 5 月 12 日受付）

■小山　覚　s.koyama@ntt.com

インターネット黎明期からサイバーセキュリティに従事し，NTT コミュニケーションズ 情報セキュリティ部長，エヌ・エフ・ラボラトリーズ 代表取締役社長を兼任し，特定非営利活動法人デジタル・フォレンジック研究会理事を務める．

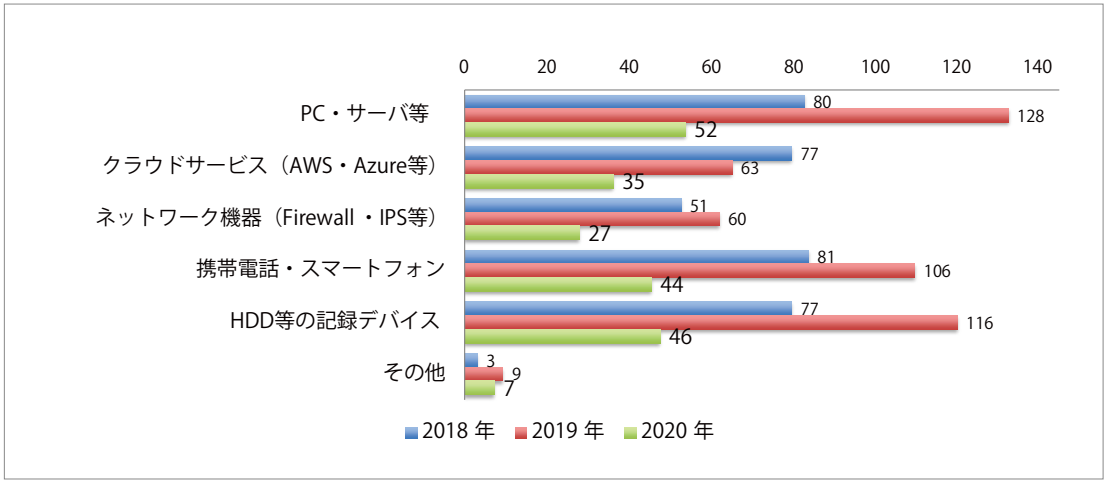

図 -4　DF の対象として思いうかべるもの

© 2021 Information Processing Society of Japan