デジタル・フォレンジックに関する調査研究

平成31年2月

一般財団法人 保安通信協会

目次

第１章　デジタル・フォレンジックに関する調査研究の概要　・・・　2

第２章　フォレンジック育成カリキュラム（基礎認定編）構築　・・・　5
　2.1　活動状況概要
　2.2　構成案検討結果
　2.3　有効性測定に向けた検討

第３章　フォレンジック育成カリキュラム（基礎認定編）講習会　・・・　14
　3.1　講習会評価・課題検討

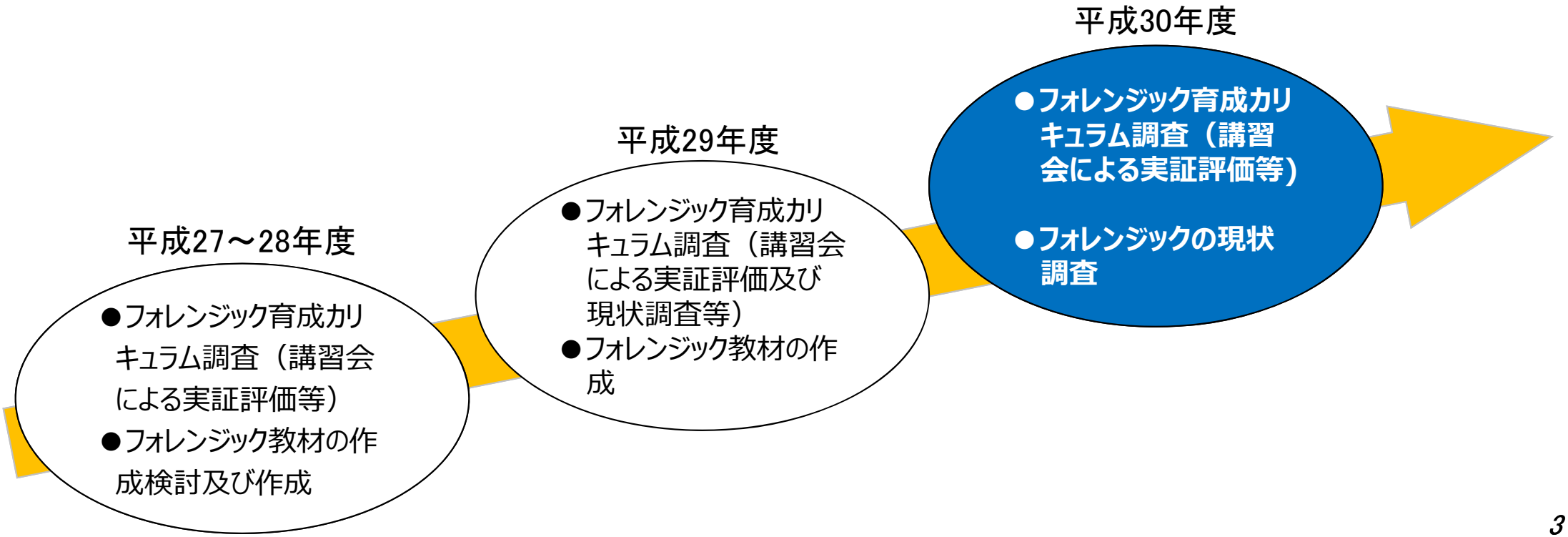
第1章　デジタル・フォレンジックに関する調査研究の概要

（1）調査分科会における調査概要及び全体の方向性

平成24年度から5カ年計画として進めてきたデジタル・フォレンジック人材育成体系概念設計検討では、デジタル・フォレンジック基礎講座（以下、基礎講座という）開設とフォレンジック教材作成という成果物を生んだ分科会活動結果となり、一定の評価結果も整ったところである。

平成29年度ならびに平成30年度では、これまでの研究活動継続に加え、現状におけるデジタル・フォレンジックの問題点や課題点の検出と、それら事項への対応／対策に関する現状調査を行っており、デジタル・フォレンジック技術初学者への情報提供や、より実務に利活用可能な情報提供を行うべく、研究活動を進めている。

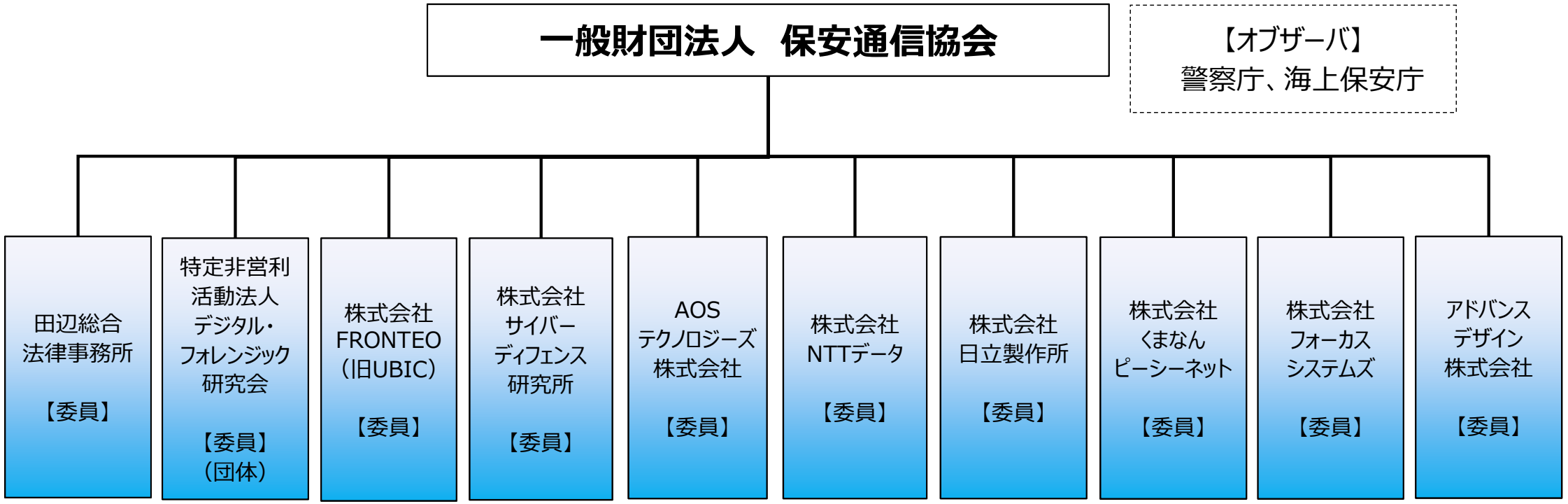
そのような中、基礎講座ついては情報提供の場やニーズ調査の場としての有効性が認められるため今後も継続的な開設とし、前年度の現状調査から得られた情報の提供の場としての活用も検討している。



(2) 調査分科会の体制

オブザーバの指導を受けながら、以下の10事業団体を委員とし、議論を行っている。

調査分科会の体制 （敬称略）

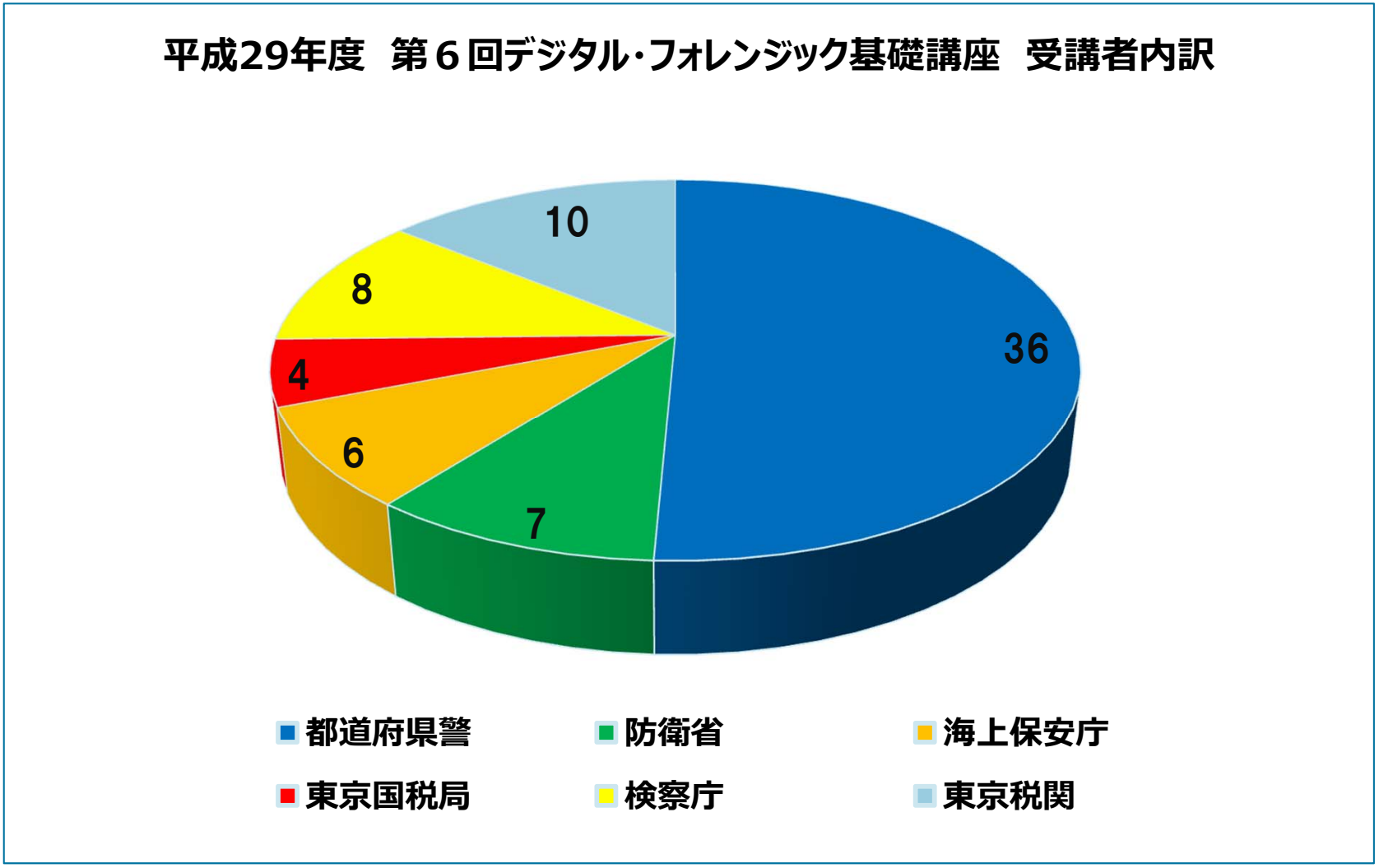


第２章　フォレンジック育成カリキュラム（基礎認定編）構築

2.1 活動状況概要

2.1 活動状況概要（1）

デジタル・フォレンジック基礎講座は、平成24年度に開講し、今年度で７回目を予定している。前回は、新たに税関職員による受講もあり、法執行機関におけるデジタル・フォレンジックに関する知識等の習得ニーズは継続して高い傾向にある。



2.1 活動状況概要（2）

前期に実施した基礎講座の実施結果等を踏まえ、フォレンジック育成カリキュラム構築に向けての実証評価を継続して行うこととし、基本構成案構築、講習会評価を行った。

基礎編カリキュラムとしての必要要件項目

項目	主な必要要件	取締機関		民間組織		教育機関
		CPDE	CDFE	EnDE	ACE	NCPS
フォレンジック基礎	コンピュータ犯罪	◎			◎	
	フォレンジックに関する法律			○		○
	フォレンジック概要	○	○		○	
コンピュータ基礎	ハードウエア構成					○
	DOS					
	ブートプロセス			○	○	
	パーテーション			○	○	
	OS		○			○
	ファイルシステム	◎	◎	○	◎	◎
証拠保全	証拠保全手法	◎	◎	○	◎	◎
	証拠品の取り扱い	◎	◎	○	◎	◎
	ハッシュ値	◎	◎	○	◎	◎
調査・分析	Windowsアーキテクチャ	◎		○	◎	
	Windowsレジストリ調査	◎	◎	○	◎	◎
	削除データ復元	○	○	○	○	○
	特殊なデータ復元（カービング）		○	○	○	
	メタデータ調査	○				
	キーワード検索	◎	◎	○	◎	○
	特殊なキーワード検索（正規表現）					
	Eメール調査	◎		○	◎	◎
	インターネットブラウザ調査	○	○	○	○	○
	パスワード解析		◎		◎	
その他	特殊ツールに関する知識		◎	○	◎	
	暗号化に関する知識	○				○
	ネットワークに関する知識		○			○
	アンチフォレンジックに関する知識					◎

フォレンジック基礎認定

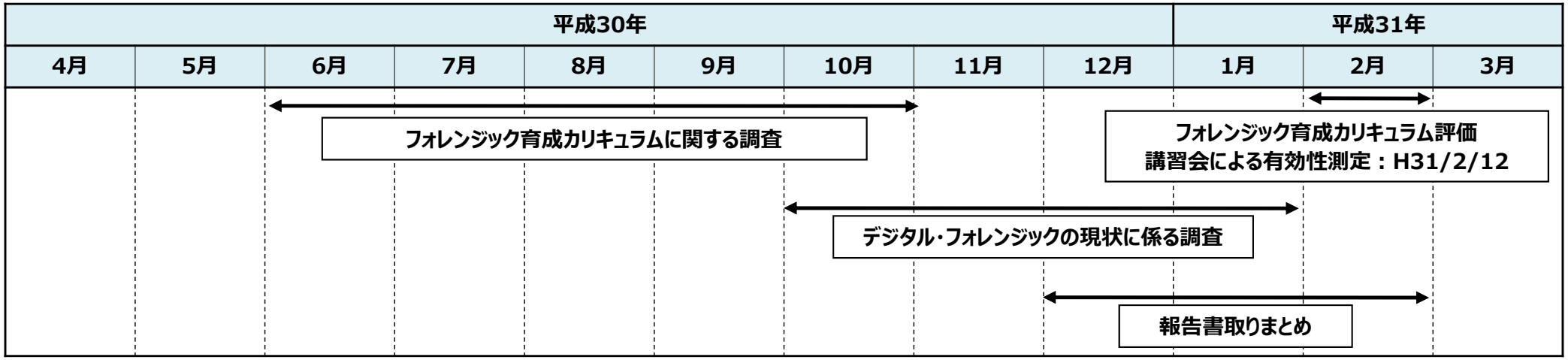
フォレンジック証拠取得者認定

フォレンジック調査官認定

作業・検討項目

- ➢デジタル・フォレンジック育成カリキュラム構成案構築
  - ・デジタル・フォレンジックに関するカリキュラム案
  - ・アンケート作成
  - ・実機を利用した操作実演
  - ・有効性測定
- ➢デジタル・フォレンジック育成カリキュラム講習会
  - ・講習会内容評価、課題検討
- ➢デジタル・フォレンジックの現状調査

スケジュール



第2章　フォレンジック育成カリキュラム（基礎認定編）の構成案構築

2.2 構成案検討結果

2.2 構成案検討結果（1）

平成29年度のフォレンジック育成カリキュラム（第六回基礎講座）の実施結果から、カリキュラム案の洗い出し・再構築を行い各項目について検討した結果、以下のとおり策定した。

■ デジタル・フォレンジック基礎に関するカリキュラム案の検討

過去6回開催した基礎講座アンケート結果から、デジタル・フォレンジックの基礎知識としての適用範囲は概ね特定できているものと考えられるが、昨年度の基礎講座アンケート結果には、フォレンジックツールの紹介や機能についての回答が多く寄せられていたことから、分科会4委員によるフォレンジックツールの利活用方法を解説するカリキュラムにすることとした。

なお、過去の基礎講座受講者の傾向として、各年度ともに一定数のデジタル・フォレンジック初学者の受講が認められるため4社によるカリキュラムには、昨年度の研究において基礎講座における固定的テーマとしたデジタル・フォレンジックの基礎的な項目と、過去の基礎講座で高い関心が寄せられたモバイル・フォレンジックに関する項目を、カリキュラムテーマとして適用とすることとした。

2.2 構成案検討結果(2)

■ 認定テスト、アンケート作成

本年度の基礎講座におけるカリキュラムでは、フォレンジックツールの利活用方法を示すものであり、習得度を計る内容のものではないため、認定テストは行わないものとする。

なお、アンケートについては、過去に実施したものを基本としつつ、本年度に実施した分科会委員によるカリキュラム構成要否や、デジタル・フォレンジック業務従事者が考える問題点や課題を挙げていただく項目を設けるものとする。

■ 実機を利用した操作実演検討

過去4カ年の基礎講座において実施したフォレンジックツール実機展示／デモは、アンケート結果からも受講者からの要望が高いことや、集客効果も見込めることが判明していることから、第七回基礎講座においても基礎講座内において時間を確保することとする。

フォレンジックツール実機展示・デモは基礎講座と同一会場内で行い、分科会委員による保全機器等の展示やデモとし、内容はデジタル・フォレンジック分科会WGで決定することとした。

2.2 構成案検討結果(3)

■ 有効性測定

カリキュラム、アンケートの各案の有効性測定、ならびに分科会委員によるフォレンジックツール等の展示やデモによる集客効果等の有効性測定を、平成31年2月12日開催の第七回基礎講座にて計ることとする。

第2章　フォレンジック育成カリキュラム（基礎認定編）の構成案再構築

2.3 有効性測定に向けた検討

2.3 有効性測定に向けた検討

平成29年度のフォレンジック育成カリキュラム（第六回基礎講座）の実施結果を踏まえ、有効性の測定方法、内容について以下のとおり検討している。

■ 第七回基礎講座案

第四回から第六回の基礎講座で開催したモバイルフォレンジック講義への高評価が多かったことから、第七回基礎講座においても講義項目に加えることとした。また第一回基礎講座開催から時間が経過していることによる、現状におけるデジタル・フォレンジックの課題の一つとされるものを講義項目とすることの必要性ならびに妥当性を計るため、講義案としての検討を行い、下記項目を選定した。

- デジタル・フォレンジックセミナー１
  - ✓ 証拠保全の現状と課題
- デジタル・フォレンジックセミナー２
  - ✓ Android調査の概要・ツール・基礎技術
- デジタル・フォレンジックセミナー３
  - ✓ オープンソースインテリジェンスによる脅威ハンティング
- デジタル・フォレンジックセミナー４
  - ✓ グローバルな犯罪対応への備え・誰でもできる高度なフォレンジック
- デジタル・フォレンジックツールを利用したデモ実演（４委員）
  - ✓ 「証拠保全データ保全＆復旧ツール」：アドバンスデザイン㈱
  - ✓ 「*Android*データ抽出・画像フォレンジック」：*AOS*リーガルテック㈱
  - ✓ 「*BelkasoftEvidence Center(*総合フォレンジックツール*)*」：㈱くまなんピーシーネット
  - ✓ 「*Lit iView XAMINER・MSAB Office(*旧*XRY)・RECON*」：㈱*FRONTEO*

第３章　フォレンジック育成カリキュラム（基礎認定編）講習会

3.1 講習会評価・課題検討

3.1 講習会評価・課題検討

「フォレンジック育成カリキュラム（基礎認定編）構築」において策定したカリキュラム、アンケート等を第七回基礎講座で実施し、下記項目における講習会としてのフィールド評価ならびにその結果の取りまとめを行うこととする。

第七回基礎講座の結果から、講習会としてのフィールド評価ならびにその結果を取りまとめ、フォレンジック育成カリキュラムや教材作成への課題整理、解決策の検討等を行う。

また、取りまとめた結果は、デジタル・フォレンジック分科会報告書として作成するものとする。

なお、第七回基礎講座に関しては、過去の基礎講座アンケート結果から無料開催を希望する声が多く上がっているため、昨年度同様に無料開催とすることとする。

- 第七回基礎講座開催概要

  開催日程：平成31年2月12日（火）10:00～17:00

  会場：東京国際フォーラム　G409会議室