一般
投稿論文

「デジタルフォレンジック実践講座」開発の取り組み

若月 里香[†1]　森 直彦[†1]　後藤 厚宏[†1]

[†1] 情報セキュリティ大学院大学

実践形式の情報セキュリティ教育に対する期待が高まっている．これを広く普及させ，継続的に質を改善していくためには，実施内容や改善の取り組みについて，事例を共有していくことが必要である．本稿では，2012 年度から 2014 年度にわたる「デジタルフォレンジック実践講座」の新規開発の取り組みについて述べる．予備的な演習と知識共有のためのディスカッションの機会を設けることで，受講者の到達レベルが向上した．

1. はじめに

生活や産業のあらゆる面にITが浸透している現在，約8万人の情報セキュリティ人材が不足しているとの報告がある[1]．社会に出て業務を始められる「実践的な」スキルを有する情報セキュリティ人材の育成は急務であり，この育成を目指す実践形式の情報セキュリティ教育の普及が期待されている．

これまで，情報セキュリティ教育における実践形式の授業は，経験をもとに形作られ，改善されてきた．しかし，その内容や改善策の共有は，十分には進んでいない．実践形式の情報セキュリティ教育を広く普及させ，継続的に質を高めていくためには，経験に頼る部分を事例として共有していくことが必要である．

ソフトウェア工学の分野では，ソフトウェア開発教育を評価するための共通問題を作成しようという取り組みがなされている[2],[3]．この中でも，成功事例／失敗事例の収集と，その共有の重要性が主張されている．

情報セキュリティ教育に関する研究では，これまで，教育内容や教授法のモデルに関する研究[4],[5],[6],[7]，教育事例の報告[8],[9],[10],[11],[12]，教材開発に関する研究[13],[14]などが行われてきた．また，情報セキュリティに携わる際に必要となるスキル[15]や，情報セキュリティ教育に関する指針を示した文書[16]等が公開されている．これらは，情報セキュリティ教育を新たに実施，または，改善する際の手がかりとして有用である．ただし，演習を主体とする実践形式の情報セキュリティ教育を対象にしたものは少ない．

本稿では，演習を主体とする実践形式のデジタルフォレンジック教育を対象に，2012年度から2014年度にわたる講座新規開発の取り組みと，それによって得られた知見を報告する．デジタルフォレンジックの実践的教育では，問題解決に向けた調査・分析力と，その土台となる多岐にわたる知識・技術を習得させる必要がある．これらの習得においては，双方を並行して習得させるのではなく，土台となる知識・技術の習得に主眼を置く予備的な演習を先に設けること，調査・分析力の向上においては，グループ内・グループ間での情報共有と議論を活性化する仕組みを設けることが有効であった．

2. 「デジタルフォレンジック実践講座」の開発と講座概要

2.1 SecCap カリキュラムの概要と育成を目指す人材像

情報セキュリティ大学院大学では，実践力のあるセキュリティ人材の育成を目指す「SecCapコース」[17]の科目として,「特設実習（セキュリティ実践Ⅰ・Ⅱ）」を設け，2012年度に「デジタルフォレンジック実践講座」を含む技術系5種類，社会科学系3種類の実践講座の開発を開始した．一部の講座は，企業の協力を得て開発，開講している．

2012年度は，一部の学生を対象にトライアル実施し，2013年度から受講者の受け入れを開始した．受講者は，修士1年生および修士2年生が中心である．実践講座の開講時期は，前期終了後の7月末から9月が中心で，集中講座形式で実施する．受講者は，前期中に，必修科目と基礎科目（選択受講）を受講することで，情報セキュリティにかかわる基本的な知識を学習済みである．

「特設実習（セキュリティ実践Ⅰ・Ⅱ）」では，「CSIRTチームで活動を始めるのに必要となる基礎的な知識・技

術，思考力を持った人材」の育成を想定している．各実践講座では，実在する題材を扱い，実際に専門家が行っているのと同等の方法で，自ら問題解決に取り組む経験を重視する．これには，インシデントの事前・事後対応に必要となる問題分析・問題解決の流れを「経験したことがある」状態で，業務のスタートラインに立ち，その後の経験や業務に特化した知識・技術をスムーズに吸収していくことのできる素地を作る意図がある．一般にインシデント対応の現場では，あらゆる可能性を網羅した完璧なマニュアルが整備されているわけではない．したがって，状況に即して能動的に考える力が必要となる．

これを座学のみで養成することは難しい．もちろん，短時間の演習で完全に身に付くものでもないが，実際の現場に近い状況で，自ら問題解決に取り組むことで，初めて分かることも少なくない．この経験が，さまざまな問題に対処する際の指針を獲得するための一助となる．

2.2　講座の目的

受講者は，「デジタルフォレンジック実践講座」において，デジタルフォレンジックの基礎を学び，デジタルフォレンジックの解析作業を実施する．デジタルフォレンジックについては，ほぼすべての受講者が未学習，未経験の状態で受講を開始する．

本講座の目的は，座学による学習とデジタルフォレンジックの解析作業を実際に行う過程で，受講者が，

①デジタルフォレンジックとはどのようなものかを知る
②ネットワーク，Web，OS，攻撃手法に対する理解を深める
③判明した事象をもとに関連する事象や全体像を明らかにしていく能力を獲得する

ことである．これらは，ひいては，インシデントが発生した際の対処における能力や忍耐，インシデントの発生を防ぐための手段に対する知見につながる．

もちろん，2.1節でも述べた通り，短時間の演習で，これらを完全に身に付けることは困難である．一方，特にデジタルフォレンジックにおいては，講座の目的③にかかわる探索的な作業が必要になり，知識・技術を身に付けているとともに，何に着目してどう考えるかという問題分析・問題解決のための思考力が重要になる．解析作業を実際に行う中で，その重要性に気付き，その思考過程を経験することは今後に活きると考える．また，小さな失敗をいろいろと経験し，試行錯誤を繰り返すことで学ぶことも多い．

2.3　教材開発と演習環境

本講座は，企業内の技術者向けに提供されていた講座を参考に，大学院向けの講座として新規に開発したものである．講座の目的，講座の時間数，受講者のレベルを考慮して，教材の難易度を設定した．

デジタルフォレンジックの解析作業を実際に行う「解析演習」の題材は，実社会での攻撃事例に沿いつつ，講座の時間数，難易度，学習効果を考慮して作成した．作成作業は，ストーリーの作成，ストーリーに沿った環境の構築，ストーリーの実行，解析対象のPCの保全という手順で行った．ストーリーは，企業における情報漏洩インシデントを想定したものである．

「解析演習」の題材作成において，具体的に考慮した点は，以下である．なお，本演習では，Windows OSを解析対象としている．

(1) Windows OSにおける一般的な調査項目をできるだけ網羅的に調査する必要が生じるような題材とする．
(2) インシデントの原因・影響が，調査によってほぼ特定できる程度の痕跡が残る題材とする．
　①攻撃者による証拠隠滅の行為は実施していない
　②解析対象のPCにおいて，Windowsファイアウォールログの設定を，破棄されたパケットのログ，正常な接続のログを取得するように設定（デフォルトではいずれも取得しないが，企業では，ウイルス対策ソフト等により，何らかの形で取得されている場合が多い）
　③解析対象のPCにおいて，NTFS[☆1]におけるタイムスタンプの更新に関する設定を，読み出し処理のみで内容の更新（書き込み）が行われなかった場合でも，Last Accessed Timeが更新されるように設定（ファイルアクセスの高速化のために，Windows Vista以降，デフォルトでは更新されない）

攻撃者による証拠隠滅や設定等により痕跡が欠損している場合には，デジタルフォレンジックの専門家が分析したとしても，一般には，必要な情報が得られるとは限らない．(2)により，デジタルフォレンジックの専門家が分析すれば，ほぼ確実に必要な情報が得られるレベルに調整している．

受講者に配布する教材としては，講義・演習資料とツール簡易マニュアルを作成した．講義資料では，デジタルフォレンジックとはどのようなものかを説明するとともに，解析作業の流れ，解析において必要となる調査項

☆1 NTFS（NT File System）：Windows系OSで使用されているファイルシステムの1つ．

目と調査方法を記載している．演習資料では，演習環境等の説明を記載している．ツール簡易マニュアルでは，各ツールの使用方法をスクリーンショットを交えて記載している．

受講者には，1人ずつ個別の解析用端末を用意し，各自がそれぞれ演習を行える環境を提供している．解析用端末には，インシデントにおいて情報の出所となった端末（「解析対象PC」）の保全イメージと解析に使用するツールが保存，インストールされている．「解析対象PC」の保全イメージは，前述のように，演習のストーリーに沿って作成した環境で実際にインシデントを発生させ，そのPCを保全したものである．解析に使用するツールは，すべて無償のもので，目的別に複数のツールを用意している．なお，「解析演習」では，「解析対象PC」の保全イメージのみを解析対象とし，「解析対象PC」以外の端末やネットワーク機器のログ等は使用しない．

2.4　講座の概要

本講座では，はじめに，デジタルフォレンジックの概要の解説を行い，その後，解析作業の流れ，調査項目と調査方法（各種ツールの使用法を含む）の説明，演習を実施する．メインの演習である「解析演習」では，受講者がデジタルフォレンジックにおける解析作業を実際に行う．

「解析演習」は，「ある企業で情報漏洩インシデントが発生した」というストーリーで実施する．受講者には，「何を目指して解析を進めるか」を示すために，「解析演習のゴール」を提示する．「解析演習のゴール」は，「ある企業で起きた情報漏洩インシデントについて，情報の出所となったと思われる端末を解析し，インシデントの原因，影響を特定する．その調査結果および判断の根拠を文書で残す」ことである．

「解析演習」のねらいは，受講者が「解析演習のゴール」到達を目指す過程において，自主的な試行錯誤をすることにより，デジタルフォレンジックの解析作業とはどのようなものかを体感すること（講座の目的①に関連），座学で学んだ調査項目や調査方法，既得の知識に対する理解を深めること（講座の目的②に関連），判明した事象をもとに関連する事象や全体像を明らかにしていく能力を獲得すること（講座の目的③）である．

2.5　「解析演習のゴール」到達に必要となる能力

「解析演習のゴール」到達には，多彩な知識と複数のツールを使いこなす技術，高い調査・分析力が必要となる．

デジタルフォレンジックの解析作業における一般的な調査・分析プロセスは，おおむね図1のようになる．図1中の→は，始点から終点方向にプロセスが進むことを表す．解析作業では，p4において判明した事象に基づき，その事象を裏付けるための調査，前後に生じた事柄を解明するための調査，見当外れであった場合の手戻りが発生する．よって，p1からp4は繰り返し行われる．このプロセスに鑑み，「解析演習のゴール」到達に必要となる調査･分析力を，「問題解決スキル」として整理する（表1）．s1 ～ s5は，p1 ～ p5のそれぞれに対応する．

また，「問題解決スキル」の土台となる知識･技術を，「知識要素」「技術要素」として整理する（表2）．「知識要素」は，「解析演習」を実施する上で必要となる知識に関する要素である．情報処理技術や情報セキュリティ分野の関連知識，および，解析作業の進め方や調査項目などデジタルフォレンジックを実施する上で必要となる専門的な知識を含む．「技術要素」は，「解析演習」を実施する際に使用するツールを使いこなす技術に関する要素である．

k1は，事前に学習されている知識であり，k2, k3, t1は，講座内で学習する．「解析演習」では，k2, k3, t1の理解･習熟を強化しつつ，s1 ～ s5を養成する．

k1は，本講座以前に開講される講義・演習により身に付けられる知識を想定している．本講座は前期終了後

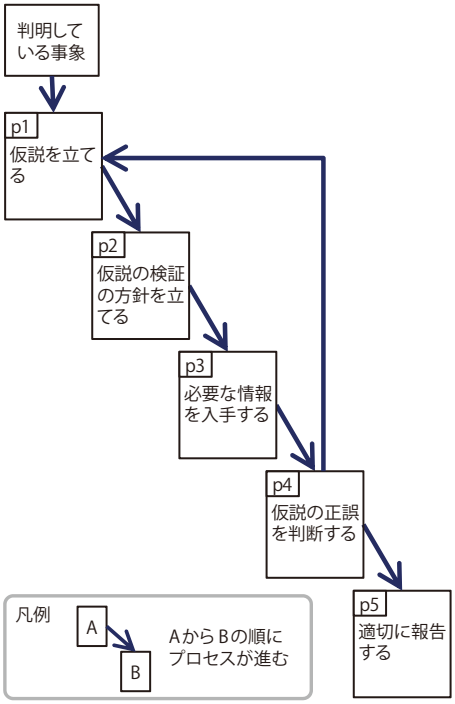


図1　解析作業における調査・分析プロセス

表 1 「問題解決スキル」

		問題解決スキル
仮説の立案	s1	仮説を立てられる． ➢ インシデント原因の仮説を立てられる． ➢ 判明した事象の裏付けとなる事柄，判明した事象の前後に生じたであろう事柄の仮説を立てられる．
仮説の検証	s2	仮説の検証の方針を立てられる． ➢ 仮説を検証するために必要な情報と手順を列挙できる． 例：仮説「USB デバイスからファイル A がコピーされた」→レジストリに記録されている USB デバイスの接続日時とファイル A の作成日時を比較
	s3	必要な情報を入手できる． ➢ 状況に応じて適切なツールとツールの機能を選択し，それを使用して必要な情報を入手できる．
	s4	仮説の正誤を判断できる． ➢ 入手した情報を元に，仮説が正しいかどうかを判断できる．
報告	s5	適切に報告することができる． ➢ 検証できた仮説，検証できなかった仮説を，判断の根拠を提示して，適切に報告することができる．

表 2 「問題解決スキル」の土台となる要素

		知識要素
事前に学習	k1	関連知識を持っている． ➢ NW，Web，OS に関する基本的な知識を持っている． ➢ セキュリティインシデントの事例，そのインシデントの仕組みの概要を知っている．
講座内で学習	k2	解析作業の流れを知っている． ➢ 解析作業の流れ：タイムラインの作成→解析基点の検討→調査方針の策定→調査（証拠固め）による事象の明確化
	k3	調査項目，調査方法を知っている． ➢ 調査項目，および，調査項目として挙げられている情報のありか，入手方法を知っている． 調査項目例：OS インストール日，アカウント情報，NW 設定，Web アクセス履歴，USB デバイス接続履歴，ファイル操作履歴，アプリケーション実行履歴 調査方法例：レジストリの HKLM¥SYSTEM¥ControlSetXXX¥Enum¥USB HKLM¥SYSTEM¥ControlSetXXX¥Enum¥USBSTORE を見ると，USB デバイスの接続日時，接続したデバイスに関する情報が入手できる．
		技術要素
講座内で学習	t1	各ツールの機能，使い方を理解している． ツール例： • Registry Decoder：保全イメージを読み込み，そこに保存されているレジストリの内容の確認や検索を行うことができる． • Autopsy：保全イメージを読み込み，その中にあるファイルの情報を始め，さまざまな情報の取得，ファイルの検索，指定したファイルのエクスポートなどができる．

に開講されるが，前期の必修科目において，ネットワーク，Web，OSの基本的な知識，一般的な攻撃と対策，セキュリティインシデントの事例等を90分×2コマ×2回の講義で扱う．また，本講座以前に開講される技術系の実践講座において，ログ解析，ネットワークセキュリティ，Webセキュリティに関連する知識・技術の習得の場を設けている．これらが，本講座で想定しているベースとなる「k1：関連知識」となる．受講者には，それぞれの知識・技術レベルを考慮して，関連する基礎科目の受講や実践講座の受講，復習を推奨することで，ベースとなるk1の習得を促している．

k2，k3，t1については，講座内で解説するとともに，受講者に配布する教材でカバーしている．たとえば，調査項目と調査方法（k3）に関しては，「解析演習」で必要となる21項目について，調査の視点，調査を通じて判明する事実，調査で使用するツール，調査対象を記述している．

2.6 「解析演習」の難易度

「解析演習」では，「解析対象PC」を解析し，インシデントの原因と影響を特定する．

ここでは，ある仮説を立案し検証する過程（1種類のp1に対するp1 ～ p4の流れ）を1サイクルとする．1サイクルは，たとえば，図2のようになる．図3は，「解析演習」において求められる解析の全体像を描いたものである．楕円は仮説，角丸四角は調査項目を表す．1つの楕円・それを始点とする1つ以上の矢印・矢印の終点となる角丸四角が1サイクルに相当する．

「解析演習」においてインシデントの原因と影響を特定するには，最小21サイクルの試行が必要である．ただし，これは，最も効率的に解析が進められた場合の数であり，実際には，解析者によって試行数は異なり，一般的に増加の方向に変化する．

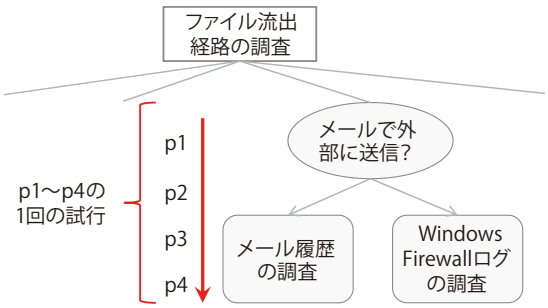
3. 受講者の状況の把握

(1) アンケートの実施

講座開始時および終了時にアンケートを実施する．アンケートは，講座前後における受講者の知識状況チェック，講座の評価（難易度，講義の仕方，受講態度等），自由記入欄からなる．

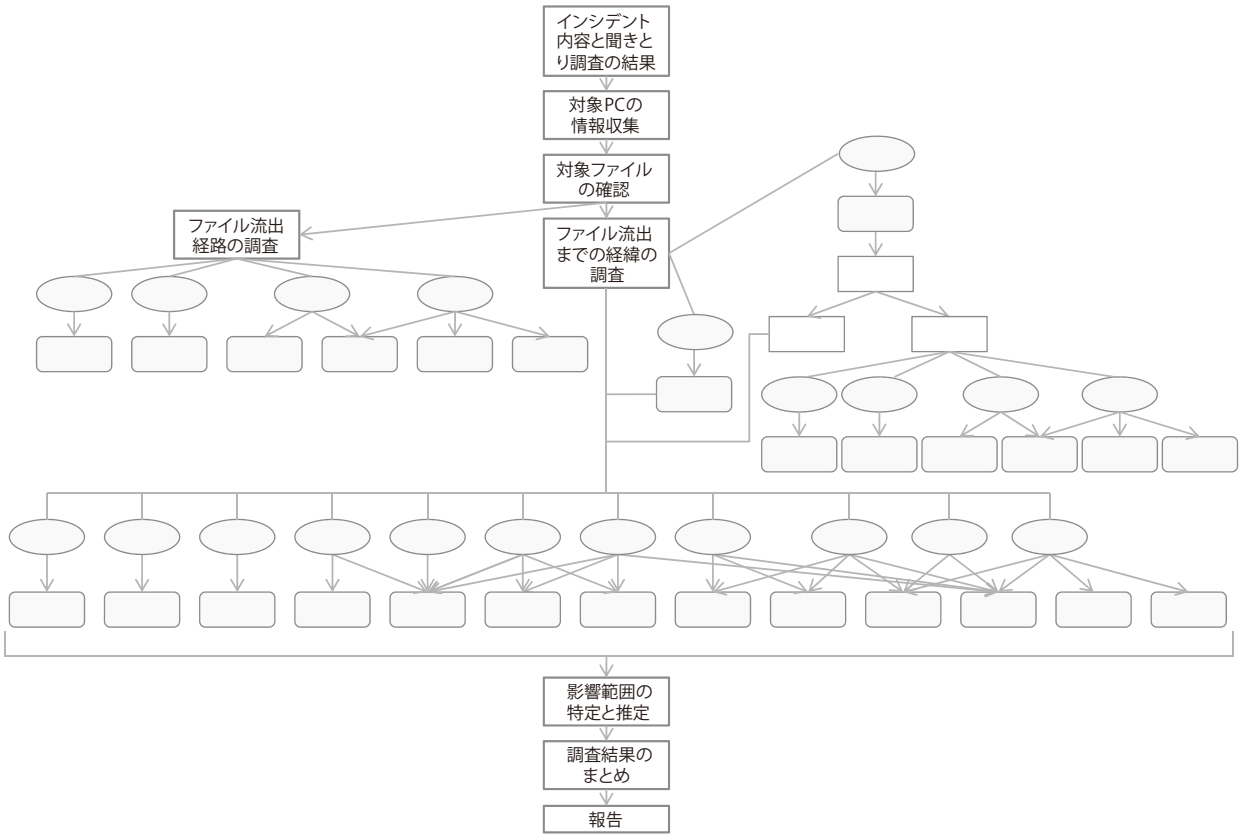
受講者の知識状況および講座の評価は，受講者の主観による5段階評価となっている．知識状況は，「1：まったく知らない」「2：知らない」「3：少し知っている」「4：知っている」「5：よく知っている」の5段階評価である．

アンケートは，4.2節，6.2節で示すように，講座終了後に分析を行い，講座内容の改善に役立てている．中でも，自由記入欄に寄せられるコメントは，改善に向けた重要な手がかりとなる．よって，講座終了時は，アンケート記入のために10分程度の時間をとり，自由記入欄へのコメントの記入を促している．ほぼすべての受



p1	「メールで対象ファイルを外部に送信した」という仮説を立てる
p2	調査の方針を立てる 調査項目：メール履歴とWindows Firewall ログ 使用するツール：Autopsy, ImDisk，MailView 調査内容：メール送信日時と対象ファイルのタイムスタンプの比較, メールの添付ファイルまたはメール本文における対象ファイルの痕跡の有無
p3	ツールを使用してメール履歴とWindows Firewallログを調査し, 必要な情報を入手する
p4	「メールで対象ファイルを外部に送信した」という仮説の正誤を判断する

図 2 「解析演習」の仮説立案・検証の 1 サイクル（図 3 より抽出）



※同じ題材を今後も使用する可能性があるため，楕円内，角丸四角内，途中の四角内の文字は削除している．

図 3 「解析演習」において求められる解析の全体像

講者が，自由記入欄に何らかのコメントを記入する傾向にある．

(2) 観察と声掛け

講座中の受講者の様子の観察と，講座中・講座前後・休憩時間の声掛けにより，受講者の状況の把握に努める．加えて，講座の様子を録画し，講座後の振り返りに利用する．

講座中は，受講者の反応や取り組みの様子を観察するとともに，質疑応答の時間をこまめに設け，その内容を記録する．また，講師とティーチングアシスタント（以下，TA）が受講者の間を回りながら声掛けを行い，受講者のフォローをしつつ，手が止まっていた個所，質疑の内容，受講者の声等を収集する．講座前後・休憩時間の声掛けは，雑談をしながら受講者の声を聞くよい機会である．

観察と声掛けの結果は，4.2 節，6.2 節で示すように，講座終了後に分析を行い，講座内容の改善に役立てている．

4. 2013 年度の実施状況と分析

4.1 実施状況

2013年度「デジタルフォレンジック実践講座」の時間割りは，表3の通りである．全体で10.5時間の講座となっている．時間割りは，「解析演習」のトライアル実施状況を参考に作成した．連続2日間の集中形式で実施している．

受講者は，出席者ベースで，36名であった．指導は，講師3名，TA1名で行った．

「解析演習」に関しては，受講者個々の取り組みと，グループワーク（グループ単位での相談および報告レポートの作成）を組み合わせる形で進めた．グループ分けは，事前に開講された技術系講座の様子や受講者の技術的背景から，各グループが同程度の力量になるよう考慮した．随時，講師が質問を受け付けるとともに，時間とタイミングを見て講師がヒントを出す（段階的に事象を公開する）ことで進捗を調整した．事象を公開する際には，併せて，その事象の調査方法を解説した．

4.2 受講者の状況の分析と課題の把握

「解析演習」中の観察と声掛けから，受講者の到達レベルは，表4のように大別された．

主にレベル1の段階でとどまっている受講者が3割程度存在した．グループ内での相談を踏まえ，レベル3に到達できていた受講者は，2割程度であった．

レベル1段階にとどまっている受講者の多くは，調査項目，調査方法（k3）に対する理解が不足している（調査項目自体が記憶されていない，各調査項目を調査する意図が理解できていないなど）傾向にあった．

グループ単位で見ると，グループ内で相談や知識の共有ができているグループと，できていないグループとが存在した．同程度の技量を有する受講者であれば，相談や知識の共有ができているグループに所属する受講者のほうが，レベル3に到達しやすい傾向にあった．

アンケート自由記入欄のコメントを分析した結果の一部を表5に示す．分類1，2のようなポジティブなコメントが多い一方，分類3，4，5のようなネガティブなコメントも多かった．

ポジティブなコメントからは，デジタルフォレンジックの専門家がやっているのと同等のことを実施できたことに意義を感じた受講者が多いことが分かった．

ネガティブなコメントの回答者の多くは，到達レベル1にとどまっていた受講者であった．分類4については，分類3，5と同時にコメントしている受講者が多かった．それぞれのツール単体でみると，使い方の難易度は，ほかの演習で使用しているツールと比較してそれほど変わらない．それにもかかわらずツールの使い方でつまずいた原因としては，使用するツールの種類が多いこと，調査項目が多いこと，それぞれの調査項目に対する理解が十分でないことなどが考えられる．

「解析演習」の演習時間については，「演習時間を長くとってほしい」というコメントと，「演習時間は長かったが難しかった」というコメントが混在していた．

「解析演習」のねらいには，受講者による自主的な試行錯誤により，座学で学んだ調査項目や調査方法に対する理解を深めること，判明した事象をもとに関連する事

表3　2013年度，2014年度講座時間割

	内容	形式	主に養成・強化する能力	時間（時）	
				2013年度	2014年度
1	デジタルフォレンジックの概要と作業の流れ，報告書	座学	k2	1.0	1.0
2	解析における調査項目と調査方法（ツールの使用方法含む）	座学演習	k2, k3, t1	2.0	1.5
3	予備演習 ※ 2014年度のみ	演習	k3, t1		6.0
4	解析演習	演習	s1 ～ s5	6.5	10.5
5	振り返り	座学		0.5	1.0
6	その他			0.5	1.0
総時間数				10.5	21.0

表4　「解析演習」における受講者の到達レベル

到達レベル	到達内容
1	仮説の立案，または，検証が不十分であり，必要な検証結果が得られていない．
2	判明している事象をもとにある事柄に関する仮説を立て，個々の検証はおおむね行えている．
3	判明している事象をもとに関連する複数の事柄に関する仮説を網羅的に立て，検証結果を得るとともに，複数の検証結果を総合的に判断することができている．

表5　2013年度アンケート自由記入欄回答割合
（回答割合の高かった5項目を抜粋）

	分類	回答割合
1	実践的で有益だった，体験して分かったことがあった	25%
2	知識の確認，新しい知識・技術の獲得ができた	28%
3	解析中に欲しい情報を見つけられなかった	11%
4	ツールの使い方でつまずいた，慣れる時間がほしい	19%
5	ついていけなかった，説明や進みが速い	25%

※寄せられたコメントを分類し，コメント数を受講者数で除した値を百分率に直し，回答割合としている．1人が複数分類のコメントを挙げている場合は，それぞれを1コメントとしてカウントしている．

象や全体像を明らかにしていく能力を獲得することの両方を含めていた．つまり，s1 ～ s5の養成における試行錯誤の中で，同時にk2，k3，t1の理解・習熟を強化することをねらった．しかし，実際には，「問題解決スキル」の土台となる知識・技術（特にk3，t1）の強化と「問題解決スキル」の養成（s1 ～ s5）を同時に行うことは厳しいという結果になった．

総じて，2013年度の講座では，講座の目的「②ネットワーク，Web，OS，攻撃手法に対する理解を深める」「③判明した事象をもとに関連する事象や全体像を明らかにしていく能力を獲得する」を満たす結果とはならなかった．主な原因は，講座内で新規に学習した内容を習熟させる仕組みが十分でなかったことである．

5. 講座内容拡充の取り組み

2013年度は，前述のように，講座の目的（2.2節）を満たすには至らなかった．2013年度の講座実施状況を受け，得られた知見は大きく次の点である．

- 「解析演習」に入る前に，k3，t1を養成するための前段階のステップが必要である．
- 「解析演習」中のグループ内での相談や知識の共有が，受講者の到達レベルを引き上げる可能性がある．

これらをもとに，2014年度は，以下のような事柄を追加で行うこととした．

- 「予備演習」を設ける
- 「解析演習」中に「中間ディスカッション」を設ける

「予備演習」，「中間ディスカッション」については，次節以降で詳述する．

全体として，「解析演習」前に「問題解決スキル」の土台となる，「知識要素」k3および「技術要素」t1の理解・習熟を強化すること，および，「解析演習」中の脱落を減らし，「問題解決スキル」の養成を補助することに力点を置いた内容となっている．

5.1 「予備演習」

「解析演習」の前に，「問題解決スキル」の土台となる知識・技術（特にk3，t1）を強化するための演習である．解析に必要となる調査項目と調査方法に関する知識（k3）を強化するとともに，各種ツールの使い方（t1）に習熟することを主な目的とする．

2013年度の経験から，「解析演習」の前に，土台となる知識・技術を実践的に使える状態に持っていくこと，そのためには，座学とともに，ツールの使い方や座学で学んだ知識が実際にどう見えるのか，どう使えるのかを，「解析演習」に近い形式での演習を通して学習させることが必要であると判断した．「解析演習」では，課題の達成に向けて探索的な作業が必要になる．土台となる知識・技術があやふやな状態では，探索空間の全体像を描けなくなるだけでなく，利用可能な事柄や技術の選択にも手間がかかり，課題の達成が難しくなる．演習を「予備演習」と「解析演習」に分けることで，それぞれの演習の主目的を明確にし，「解析演習」では，「問題解決スキル」の養成（s1 ～ s5）に注力できる状況を作り出す．

「予備演習」では，解析対象のPCにおいて，何が起きたか，どのような操作が行われたかが分かっている状態で，その痕跡を見つけ出す．

「予備演習」用に新たに準備した教材は，以下の2つである．

- 予備演習用保全イメージ
- 予備演習用演習シート

予備演習用保全イメージは，予備演習用のストーリーを作成し，そのストーリーに沿って操作した予備演習用解析対象PCを保全したものである．予備演習用演習シートは，予備演習用解析対象PCの操作内容と，その操作の痕跡を見つけるのに適したツールを，操作内容ごとに記載したものである．受講者は，操作が実施された時刻と見つかった痕跡の内容等を穴埋め式に記述していく（図4）．

「予備演習」の冒頭では，ツールの使い方の説明を兼ねて，講師とともに数個の項目を一緒に調査する時間を設ける．その後は，解説と各自による作業を交互に行う．終わりに，「予備演習」全体の解説と，解説を受けての確認と振り返りを行う．演習中は，講師とTAが受講者の間を回り，質疑応答とフォローにあたる．

演習シートで挙げている操作内容の一部を，表6に示す．全部で29個の操作内容を用意している．これらの操作内容の痕跡を明らかにしていくことで，「解析演習」で実施する必要のある21サイクル（2.6節）の試行のうち，9サイクル相当を繰り返し練習できるように設計している．この9サイクルの試行では，「解析演習」全般の試行にかかわる主要な調査項目（例：Webアクセス履歴，USBデバイス接続履歴，アプリケーション実行履歴）に対する調査を実施する．

「予備演習」を「解析演習」との対比で見ると，調査によって明らかにすべき事象が明確になっている状態（p1が固定されている状態）で，それぞれの痕跡を見つけ出すための検証の方針を立て（p2相当），必要な情報

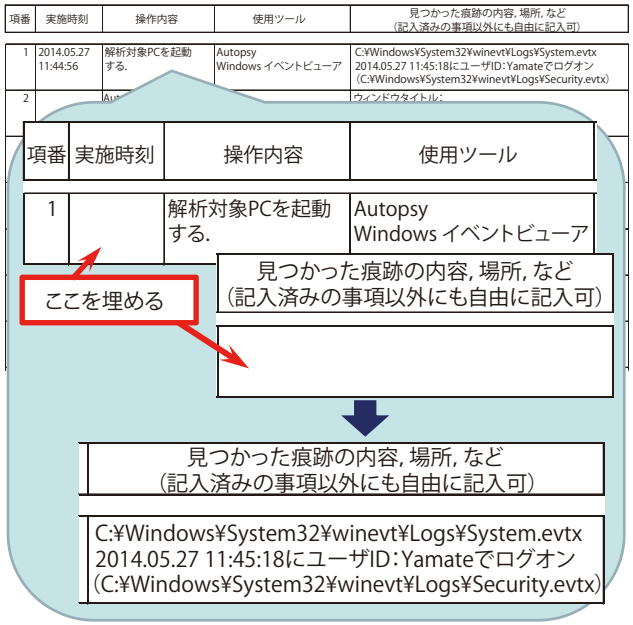


図 4　予備演習用演習シート

表 6　予備演習用演習シート項目例

操作内容	使用ツール
Adobe Reader のダウンロードページを検索エンジンで検索する	Autopsy
Adobe Reader をダウンロードする	Autopsy
Adobe Reader のインストール完了	Autopsy Windows イベントビューア
USB メモリを解析対象 PC に接続する	USB Deview Registry Decoder
メモ帳で「ToDo-0527.txt」を開く	Autopsy
「ToDo-0527.txt」に追記して保存する	Autopsy
メールを送信する	MailView
「ProductSales.docx」をゴミ箱に入れる	Autopsy

を入手する（p3）練習と見ることができる．「解析演習」では，多くの不確定要素が存在する中で，仮説（何を明らかにするか）や解析の方向性を自力で決めねばならない．「予備演習」では，これを固定することで，複雑さを軽減し，穴埋め問題を解く要領で，k3 と t1 を練習によって強化する．予備演習用のストーリーは，主要な調査項目とツールの使用を，繰り返し確認できるように作成している．受講者は，「予備演習」に取り組むことにより，座学で学習した主要な調査項目に関する知識を確認し，調査方法とツールの使い方に習熟することが期待される．「予備演習」を実施することで，「解析演習」の前に実施する座学に対する演習の時間比は，2：1 程度から 1：3 程度にまで大幅に増加する．

5.2　「中間ディスカッション」

「解析演習」において，解析の途中経過を共有し，議論する場として，「中間ディスカッション」を設ける．「中間ディスカッション」は，グループ内ディスカッションと全体ディスカッションで構成し，グループ内ディスカッションを実施した後，全体ディスカッションを実施する．

「中間ディスカッション」を設けた意図は，次の通りである．

- グループ内ディスカッションによる知識の共有や整理を通じて気付きを得，理解を進める．また，その過程におけるグループメンバ間での教え合いや講師との質疑を活発化する．
- 全体ディスカッションにより，グループ間で途中経過の共有を行い，出された事柄について議論・検討することで，気付きを得，理解を進める．
- これらにより，「解析演習」中の脱落を減らすとともに，全体の足並みをそろえる．

「中間ディスカッション」は，「解析演習」中に 3 回設ける．各回のディスカッションテーマは，事前に周知しておく．全体ディスカッションの実施前には，判明した事象，調査の過程，不明点，残作業をグループ内で整理する．この間，講師が各グループを回り，質疑応答をしつつ状況を確認する．全体ディスカッション中は，講師は，議論の活性化を促すとともに，議論の中で，受講者が解析の方向性を得られるよう誘導する．

同じ程度の技量を有する受講者であっても，興味関心の違いなどにより，目の付けどころや発想は変わってくる．「中間ディスカッション」による知識の共有やアイディアの交換は，新たな気付きを生み，解析を進める上で，補助的な役割を担うことが期待される．

また，受講者ごとに能力差はあり，「知識要素」k3 の理解・習熟にもバラつきがある．このバラつきは，受講者間の差でもあり，調査項目が多岐に渡ることに起因する受講者自身の得意分野･不得意分野の差でもある．「中間ディスカッション」では，受講者個々が持つ知識を寄せ集め，補い合う効果が期待される．

6.　2014 年度の実施状況と分析

6.1　実施状況

2014 年度「デジタルフォレンジック実践講座」の時間割りは，表 3（4.1 節）の通りである．全体で 21 時間の講座となっている．連続 2 日間×2 週の集中形式で実

施している．

受講者は，出席者ベースで，32名であった．指導は，講師5名，TA1名で行った．

「解析演習」に関しては，受講者個々の取り組みと，グループワーク（グループ単位での相談および報告レポートの作成）を組み合わせる形で進めた．また，前述の通り，「中間ディスカッション」を3回実施した．各回の全体ディスカッションの時間は，30分程度である．グループ分けは，事前に開講された技術系講座の様子や受講者の技術的背景から，各グループが同程度の力量になるよう考慮した．その際，各グループ内での議論を活発にするため，グループ内に少なくとも2名は同程度の高い技術力を有する者を配置する，もしくは，中程度の技術力を有する者4名でグループを構成するよう努めた．

6.2　受講者の状況の分析と実施内容の分析

「解析演習」における受講者の到達レベルは，主にレベル1（4.2節表4）の段階でとどまっている受講者は，2013年度の3割程度から1割未満に減少し，レベル3に到達できていた受講者は，2013年度の2割程度から6割程度に増加した．アンケート自由記入欄に寄せられたコメント回答割合は，表7のように変化した．分類1，2のようなポジティブなコメントが多くなり，分類3，4，5のようなネガティブなコメントが減少した．また，講座前後における知識状況評価においては，講座前に3以下を回答した受講者のうち，講座後に4以上を回答した受講者の割合が図5のようになった．設問内容，選択肢，および，自己評価であるという性質上，大きな変化とはなっていないが，2013年度に比べて，講座後に4以上に達した受講者の割合が増加した．

グループ単位で見ると，「中間ディスカッション」が契機となり，グループメンバ間の相談や知識の共有が，ほぼすべてのグループで活発に行われていた．ややおとなしいグループも存在したが，講師が声掛けをすることで，議論の活性化を促した．全体ディスカッションについては，必要な情報のやり取りはされていたが，より活性化することで，学習効果が高まると思われる．

観察と声掛けをもとに評価した到達レベルおよびアンケートの結果から，2014年度に追加実施した内容は，意図した効果を上げ，「問題解決スキル」の土台となる知識・技術の習熟を強化し，「問題解決スキル」の養成に効果的であったと推測される．また，全体として，講師との質疑も多くなり，受講者の取り組みが活発になっていた．総じて，2014年度の講座では，改善の余地はあるものの，講座の目的（2.2節）を実現するための体制が構築できたと考えている．

表7　アンケート自由記入欄回答割合

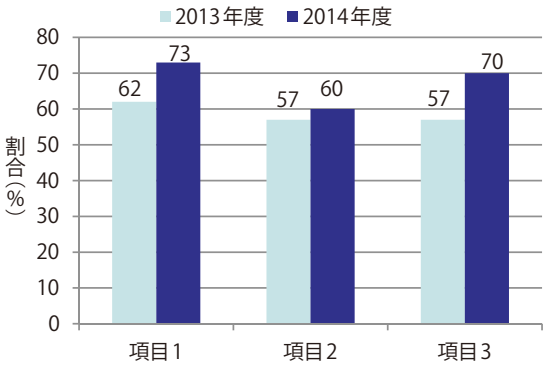
	分類	2013年度	2014年度
1	実践的で有益だった，体験して分かったことがあった	25%	47%
2	知識の確認，新しい知識・技術の獲得ができた	28%	28%
3	解析中に欲しい情報を見つけられなかった	11%	3%
4	ツールの使い方でつまずいた，慣れる時間がほしい	19%	6%
5	ついていけなかった，説明や進みが速い	25%	0%

7.　まとめ

本稿では，2012年度から2014年度にわたる，「デジタルフォレンジック実践講座」新規開発の取り組みを報告した．

本講座の目的は，座学による学習とデジタルフォレンジックの解析作業を実際に行う過程で，受講者が，「①デジタルフォレンジックとはどのようなものかを知る」「②ネットワーク，Web，OS，攻撃手法に対する理解を深める」「③判明した事象をもとに関連する事象や全体像を明らかにしていく能力を獲得する」ことである．

講座内で実施している「解析演習」では，実社会での



項番	履修項目	内容
項目1	解析手法	解析基点，タイムライン
項目2	解析項目（1）	レジストリ，イベントログ，プリフェッチファイル
項目3	解析項目（2）	Webアクセス履歴，Windows Firewallログ，USB接続履歴

※　割合＝（講座前3以下かつ講座後4以上回答者数）／（講座前3以下回答者数）＊100

図5　アンケート知識状況評価において，講座前に3以下を回答した受講者のうち，講座後に4以上を回答した受講者の割合

攻撃事例に沿った題材を用意し，デジタルフォレンジックの専門家が実際に行っているのと同等の解析作業を演習として実施している．「解析演習」では，探索的な作業を行うことが求められる．また，「解析演習」を行う前には，その土台となる知識･技術の習熟が必要である．

2013年度においては，解析を実施する上で土台となる知識・技術の習熟が不十分で，「解析演習」が十分に行えなかった受講者が3割程度に達した．2013年度の経験から，「解析演習」に入る前に，土台となる知識・技術を実践的に使える状態に持っていくこと，そのためには，座学とともに，ツールの使い方や座学で学んだ知識が実際にどう見えるのか，どう使えるのかを，「解析演習」に近い形式での演習を通して学習させることが必要であると判断した．そこで，2014年度には，演習を通して必要な知識・技術を学ぶ「予備演習」を実施した．

「予備演習」は，あとで行う解析作業を受講者が想定できる形式で，かつ，複雑さを軽減し個々の知識・技術の習熟に主眼を置いた形式で実施した．「予備演習」を実施することで，「解析演習」の前に実施する座学に対する演習の時間比は，2：1程度から1：3程度まで大幅に増加した．予備演習は，基本的に個人演習であるが，講師やTAが密にサポートすることで効果をあげている．

演習を「予備演習」と「解析演習」に分ける理由は，土台となる知識･技術があやふやな状態では，「解析演習」を円滑に行うことが困難なためである．「解析演習」では，課題の達成に向けて探索的な作業が必要になる．前者があやふやだと，探索空間の全体像を描けなくなるだけでなく，利用可能な事柄や技術の選択にも手間がかかり，課題の達成が難しくなる．

「解析演習」ではグループ学習が重要な意味を持つ．複数人で議論することにより，個々の知識の不足を補ったり，1人ではなかなか思いつかない可能性に至ったりすることができる．2014年度からは「中間ディスカッション」を導入した．グループ内・グループ間の情報共有と議論を活性化するとともに，グループ間での進捗の足並みをそろえる効果をねらったものである．

以上の経験をまとめると，以下のようになる．

- 実践的な「解析演習」とその土台となる知識・技術の習得を並行して行うのは困難である．最初に土台を固めないと，「解析演習」が迷走して進まなくなる可能性がある．
- 実践的な「解析演習」の前に，その土台となる知識･技術の習得に十分な時間をかける必要がある．土台となる知識・技術の習得は，座学と演習の両方を実施し，その時間の多くを演習に割り当てることが有効である．演習は，後で行う解析作業を受講者が想定できる形式で，かつ，複雑さを軽減し個々の知識･技術の習熟に主眼を置いた形式とするのがよい．
- 「解析演習」を単純なグループ学習として行うだけでは，情報共有がうまく行えなかったり，グループによる差が大きくなったりする可能性がある．グループ内・グループ間の情報共有と議論が活発に行われる仕組み作りが必要である．

謝辞　本講座は，NTTセキュアプラットフォーム研究所との情報セキュリティ人材育成プログラムに関する共同研究の一環として開発，開講している．

参考文献

1) 情報セキュリティ政策会議：サイバーセキュリティ戦略（2013），http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf（2015年2月9日現在）
2) 権藤克彦：ソフトウェア開発教育における共通問題，情報処理，Vol.54, No.9, pp.898-902 (Sep. 2013).
3) 井垣　宏，奥田　剛，細合晋太郎，早瀬康裕：PBLと共通問題，情報処理，Vol.55, No.10, pp.1064-1068 (Oct. 2014).
4) 内田勝也：技術者・管理者向け情報セキュリティ教育試案，日本セキュリティ・マネジメント学会誌，第15号，pp.30-40 (2003).
5) 松村真木子：情報セキュリティに敏感な一般エンドユーザ養成へ向けて，情報処理学会論文誌，Vol.48, No.9, pp.3183-3192 (2007).
6) Idziorek, J., Rursch, J. and Jacobson, D.: Security Across the Curriculum and Beyond, Proceedings of 2012 Frontiers in Education Conference, pp.1-6 (2012).
7) 増山一光：高校生に対する情報セキュリティ教育の教授法に関する研究，博士論文 (2013).
8) 佐々木良一：東京電機大学における情報セキュリティ教育，電子情報通信学会技術研究報告，SITE，技術と社会・理論，Vol.104, No.392, pp.7-12 (2004).
9) Peterson, G. L., Raines, R. A. and Baldwin, R. O.: Graduate Digital Forensics Education at the Air Force Institute of Technology, Proceedings of the 40th Annual Hawaii International Conference on System Sciences, 264c (2007).
10) Dimkov, T., Pieters, W. and Hartel, P.: Training Students to Steal: A Practical Assignment in Computer Security Education, Proceedings of the 42nd ACM Technical Symposium on Computer Science Education, pp.21-26 (2011).
11) 西村浩二，大東俊博，岩沢和男 他：広島大学における情報セキュリティ・コンプライアンス教育の取組み，情報処理学会研究報告，Vol.2012-IOT-18, No.2, pp.1-6 (2012).
12) 増山一光，佐藤　直：学校設定科目によるコンピュータウィルス対策教育の実践，日本教育情報学会学会誌，Vol.27, No.3, pp.15-25 (2012).
13) 原田晶子，植田祐史，隅谷孝洋，中村　純：オンライン情報セキュリティ教材の開発，情報教育シンポジウム2005論文集，pp.149-150 (2005).
14) 川上昌俊，安田　浩，佐々木良一：情報セキュリティ教育のためのeラーニング教材作成システムELSECの開発と評価，情報処理学会論文誌，Vol.52, No.3, pp.1266-1278 (2011).

15) 情報処理推進機構：IT スキル標準 V3 2011（2012）, http://www.ipa.go.jp/jinzai/itss/download_V3_2011.html（2015 年 2 月 9 日現在）
16) 日本ネットワークセキュリティ協会：情報セキュリティ教育の指導者向け手引書（2007 年版），http://www.jnsa.org/result/2007/edu/materials/071111/（2015 年 2 月 9 日現在）
17) enPiT-Security【SecCap】分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野），http://www.seccap.jp/（2015 年 3 月 31 日現在）

若月 里香（正会員）wakatsuki@iisec.ac.jp
2013 年情報セキュリティ大学院大学博士前期課程修了．2013 年より SecCap コース技術系実践講座のサポート業務に従事．2014 年より情報セキュリティ大学院大学特任助手．

森 直彦（正会員）n.mori@iisec.ac.jp
1984 年京都大学大学院工学研究科情報工学専攻修士課程修了．現在，NTT アドバンステクノロジ（株）にて企業のセキュリティ向上に資するセキュリティサービス・コンサルティングビジネスのグループを主管．特定非営利活動法人日本ネットワークセキュリティ協会幹事．2012 年より情報セキュリティ大学院大学客員教授．

後藤 厚宏（正会員）goto@iisec.ac.jp
1984 年東京大学大学院工学系研究科情報工学専攻博士課程修了（工博）．NTT 研究所にてインターネットセキュリティ技術, 高信頼クラウドコンピューティグ技術の研究開発等に従事．2011 年より情報セキュリティ大学院大学教授．本会フェロー．本会理事．IEEE Computer Society Board of Governor.

投稿受付：2015 年 4 月 9 日
採録決定：2016 年 1 月 21 日
編集担当：柴山悦哉（東京大学）