

**高度IT人材育成システム開発事業
(ITSS実証実験)
「ケースメソッドによる
セキュリティスキルアップ教育」**

**松田 剛
株式会社ヒューコム**

2004年5月18日

第一部 プロジェクト概要

「高度IT人材育成システム開発事業」



平成14年度経済産業省の補正予算事業。経済産業省がすすめる、高度IT人材を育成するためのITスキル標準(ITSS)に準拠した人材育成システム開発とその評価・実証を通じ、効率的な育成方法・スキームを示していくことを目的とする。

採択先(計30社)

- ・ (株)学習研究社 「問題解決ノウハウの顕在化と共有による実務能力開発」
- ・ 慶応義塾大学 「産学協同学生/高度IT人材育成プログラムの地域展開」
- ・ 仙台ソフトウェアセンター 「顧客の問題解決を図る提案型営業ができる技術者の養成」
- ・ 松下電器産業(株) 「コミュニティーデータセンタスキル標準化とIT産業育成」
- ・ 浜名湖国際頭脳センター 「効率的、効果的な高度セールス人材育成システムの検証」
- ・ 日本ネットワークセキュリティ協会 「ケースメソッドによるセキュリティスキルアップ教育」
- ・ 他24団体

「ケースメソッド」式情報セキュリティ教育の実践 及びその検証

「ケースメソッド」(ケーススタディ、課題解決型教育手法)・・・主に米国ビジネススクールにて実践されている課題解決型の教育手法

従来型の教育手法(知識賦与教育、ナレッジ教育、暗記重視型教育)の弊害を克服し、「ものを考える」教育の実践及びその効果を測定する。

(ケースメソッド手法は、主にハーバードビジネススクール及び慶応ビジネススクールを参照した)

背景及び問題意識 1



情報セキュリティ分野の特質と問題点 1

概念が抽象的で人によってその捉え方が違う

例えば発注側と受注側、経営者と技術者、開発系と構築系など立場の違いにより、「情報セキュリティ」に対する捉え方が異なりコミュニケーションが成立しない。

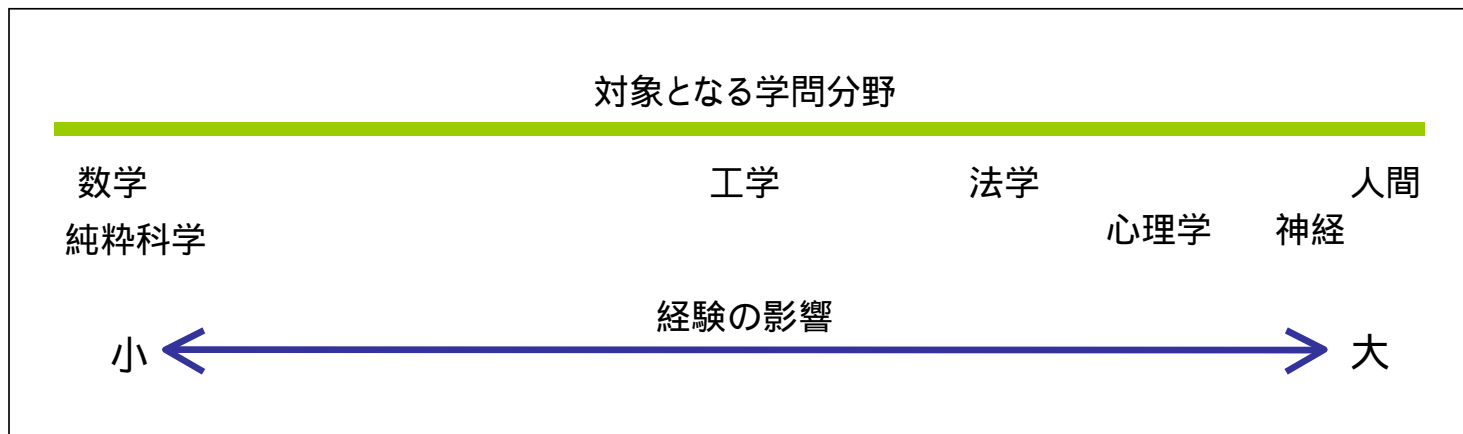
プロジェクトの失敗やトラブルは、コミュニケーションギャップが問題の根底にある場合が多い。

背景及び問題意識 2



情報セキュリティ分野の特質と問題点 2

対象となる範囲が広い



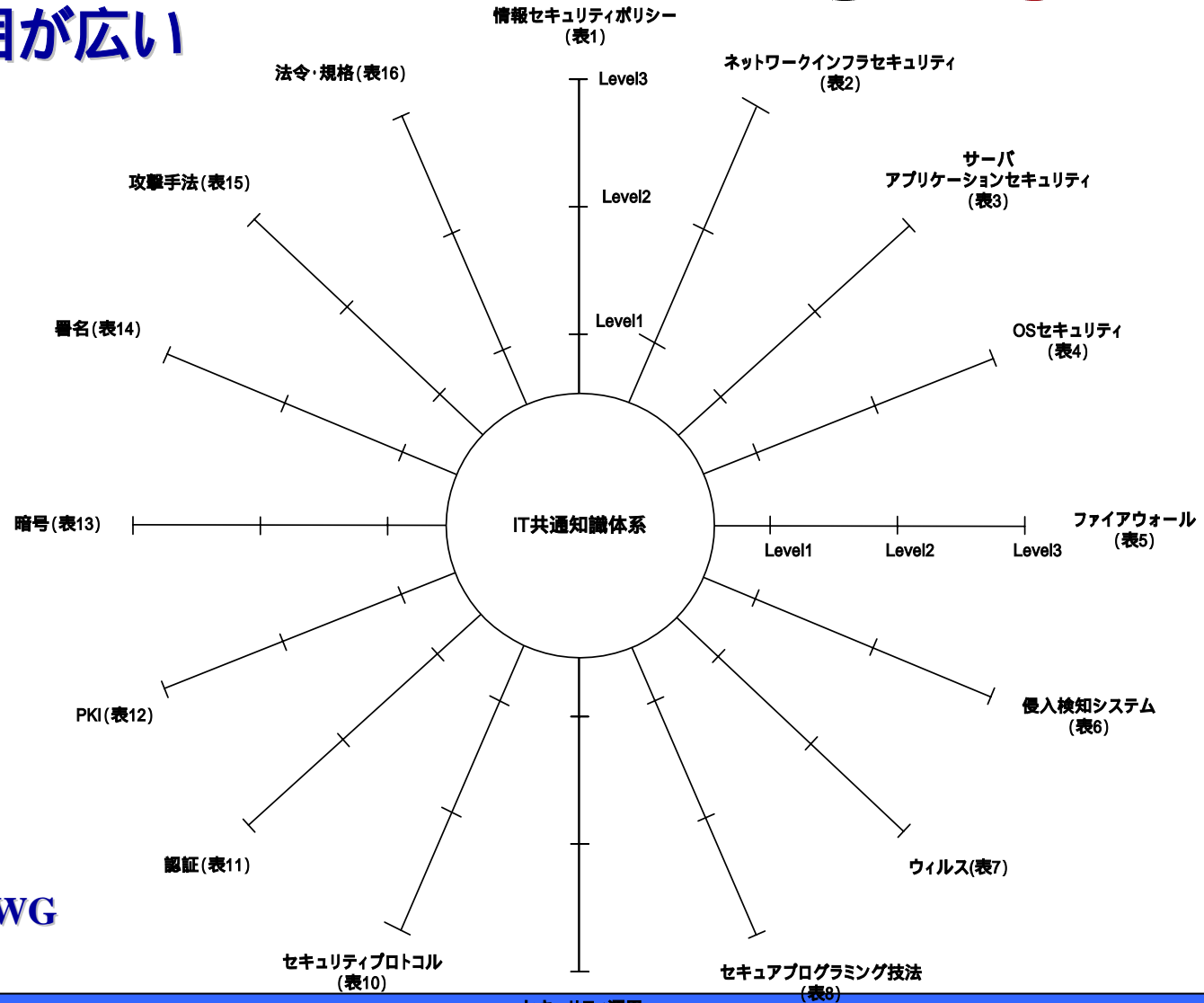
純粋科学としての数学に始まり、法学、経済学、経営学、心理学、神経から人間そのものの知識へと広がる（情報セキュリティ = 総合科学）

背景及び問題意識 2



対象となる範囲が広い

技術分野だけでも...



教育部会 Skillmap作成WG
2002年度策定

背景及び問題意識 3



情報セキュリティ分野の特質と問題点 3

現在提供されている教育サービスの問題点

情報セキュリティ教育と謳っても、Firewallのプロダクト講習や暗号理論(数式)の講義など、「各論分野の知識賦与教育」がほとんど。製品オリエンテッドな技術者育成、研究者育成は充実しているものの、情報セキュリティ分野全体を俯瞰、鳥瞰させる教育サービスが提供されていない。

背景及び問題意識 4



情報セキュリティ分野の特質と問題点 3

分野全体を俯瞰・鳥瞰させることの重要性

「情報セキュリティは製品ではない。一連のプロセスである」

個別分野の専門家、製品オリエンテッドな技術者だけでは、必ずしも組織全体のセキュリティレベル向上に寄与できるとは言えない。

「プロセス」として捉えられる人材が求められている。

- 1) 他分野の職種又は立場(視点)の違い、その相互理解
- 2) 情報セキュリティ分野を包括的に理解した人材の育成、輩出
- 3) 従来型の知識偏重教育ではなく、問題解決能力、企画構想力、リーダーシップ等の能力開発を重視しより実務的な教育を目指す。

ケースメソッド方式とは

20世紀初頭ハーバード・ビジネススクールにて開発された教育手法
伝統的な講義形式の授業と大きく異なり、受講者はケース(事例が記述された冊子)を元にディスカッションをしながら授業をすすめていく方式。

「HBS(1)が真っ先に強調するいちばん大切な視点は、ゼネラル・マネジメント(総括経営)の視点である。もちろん、生産、労使関係、人事、財務、教育訓練、その他諸分野における専門的手法を軽視しているわけではない。そうではなくて、トップ経営者に要求される最大の職務は、組織の各機能をいかに調和をもって統合し運営するかという点だと主張しているのである。…中略…経営諸領域の機能そのものよりも、それらを全体として捉えることに重点をおいている」(2)

その方法論として、「ケースメソッド」が採用されている。

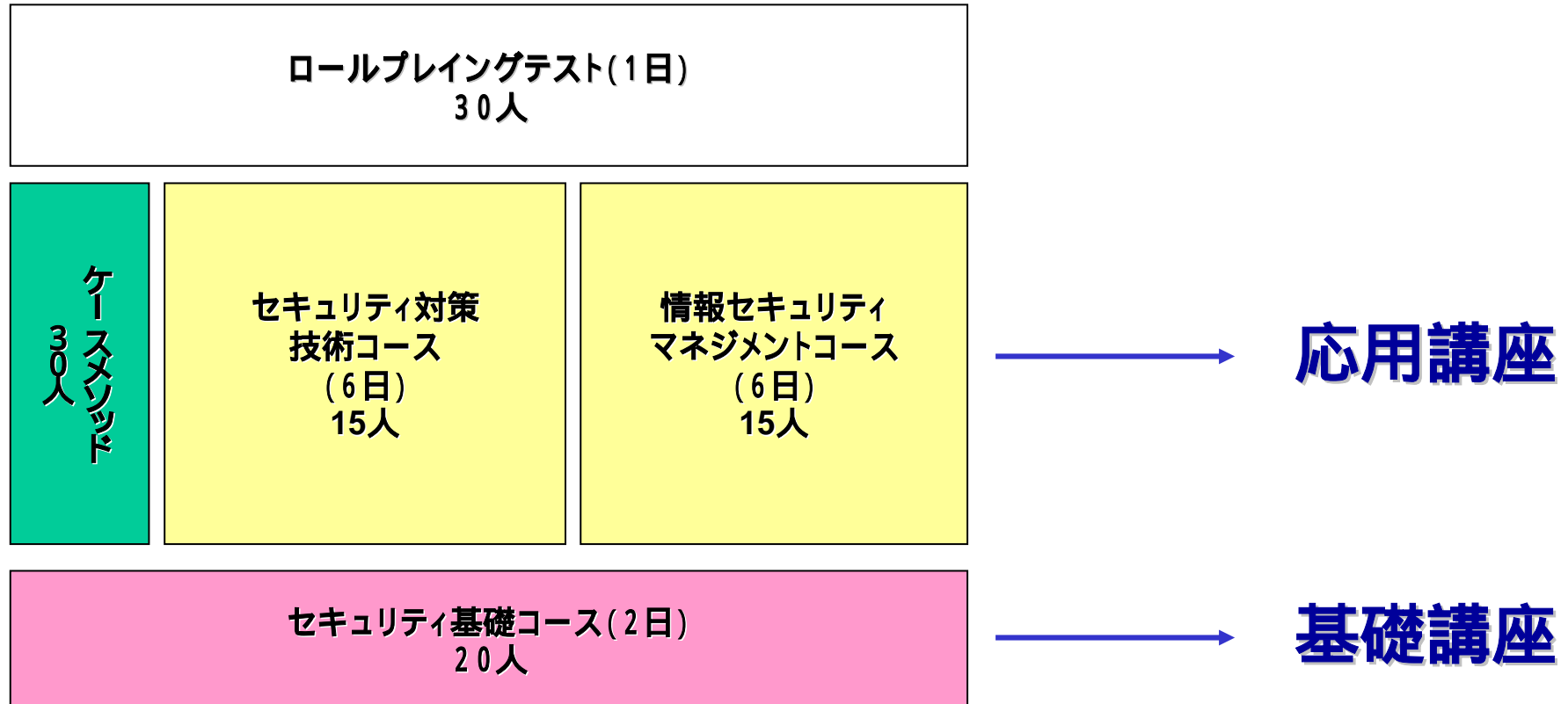
1 HBS:ハーバード・ビジネススクール

2 ハーバード・ビジネススクールの経営教育:デイビット・W・ユーイング著 1993TBSブリタニカ

「ケースメソッド式情報セキュリティ教育」を展開しその有効性を評価する。

第二部 カリキュラム概要

コースウェア



**受講者総数:30人、期間:9月27日～11月1日、
講義日数:9日、講義時間:約55時間**

カリキュラム (基礎コース)



コース名	実施担当	教育目的及びその手法	実施日程	カリキュラム
セキュリティ 基礎コース	SEA/J	基礎知識習得 (ナレッジ教育) 座学	9月20日(土) 9月21日(日) 9:00~18:00 終日を予定	<ol style="list-style-type: none"> 1、ネットワークセキュリティ (TCP/IP、Router、FTPサーバと脆弱性・・・) 2、攻撃手法(WHOIS、パスワードクラック、ポートスキャン・・・) 3、ファイアウォール(Routingとアクセス制御、パケットフィルタリング・・・) 4、侵入検知システム(検出方法、プロミスキャスモード・・・) 5、認証・暗号(ユーザ認証、メッセージ認証、共通鍵暗号) 6、PKI(公開鍵暗号方式、RSA暗号方式、電子証明書) 7、セキュリティプロトコル(SSL、Ipsec、RADIUS・・・) 8、ウイルス(ファイル感染、分類方法、検出技術) 9、クライアントセキュリティ(ブラウザセキュリティ、JavaScript、ActiveX・・・) 10、権限とデータ管理(ユーザ管理、NULL接続の制限、権限設定) 11、情報セキュリティポリシー(スタンダード、プロシージャ、情報資産の洗い出し) 12、スキルチェック試験

日数 : 2日間、時間 : 終日(8時間程度)、
試験:有り(受講前、修了後スキルチェック試験実施)

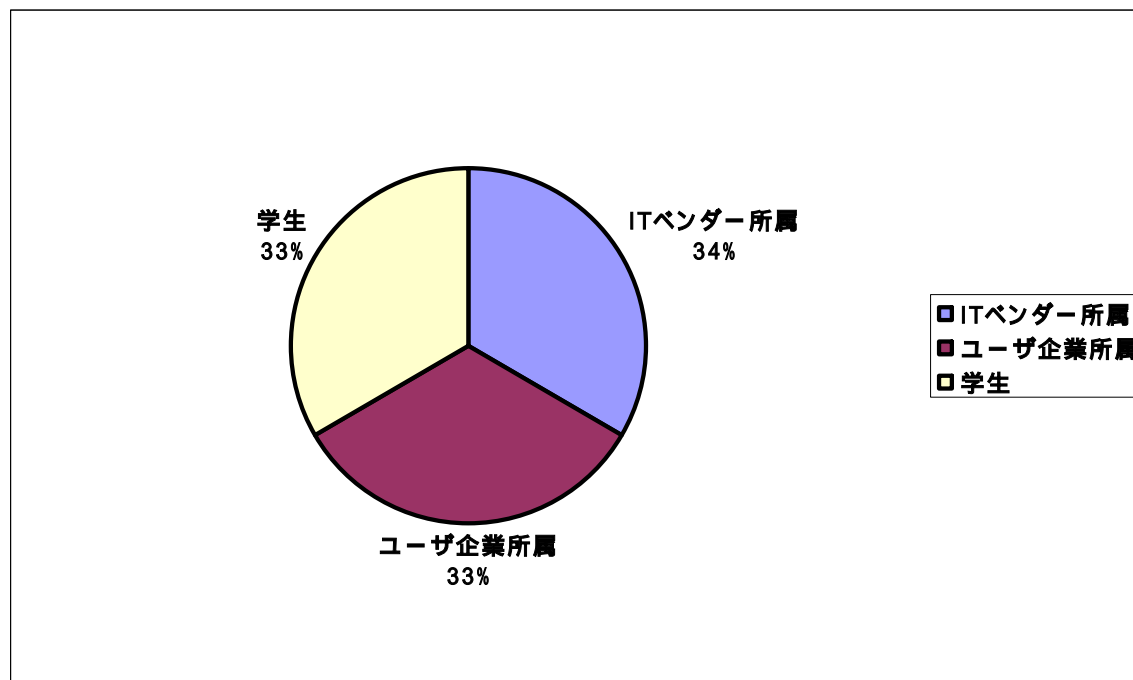
カリキュラム(応用コース)



コース名	実施担当	教育目的及びその手法	実施日程	カリキュラム
セキュリティ技術対策コース (応用コース)	ヒューコム	セキュリティ技術の応用知識習得 (ナレッジ教育) 座学・実習	9月27日(土) 10月4日(土) 10月11日(土) 10月12日(日) 10月18日(土) 10月25日(土) 13:30~16:30	1、社内ネットワークでの脅威 不適切なアクセス制限、なりすまし、盗聴、その他脅威(無線LAN、情報漏えい) Windowsセキュリティ (認証、PKI、OSセキュリティ、ウイルス、攻撃手法…) 2、外部からの侵入 脅威の理解、予防対策、検知、事後対応 (OSセキュリティ、サーバセキュリティ、セキュリティプロトコル、Firewall…)
ケースメソッド式グループディスカッション (応用コース)	・技術評価WG ・ディアイティ ・ヒューコム	ケース(課題)解決 (グループディスカッション) 6人1グループ (合計30人5グループ)	日程は同上 16:30~18:30	ケース策定 (セキュリティ技術対策コース、セキュリティマネジメントコースと合同で実施) (1つのケースを期間終了までに解決する)
セキュリティマネジメントコース (応用コース)	ディアイティ	セキュリティマネジメント手法の応用知識習得 (ナレッジ教育) 座学	日程は同上 13:30~16:30	1、情報セキュリティ概論 2、リスク分析手法(基礎) 3、リスク分析(詳細リスク分析マネジメント) 4、情報セキュリティポリシ概論 5、情報セキュリティポリシ策定 6、情報セキュリティ関連法規

受講者の性質

受講者の所属先比率



受講者全体(=30人)で、ITベンダ所属(システム受注側)10人、ユーザ企業(システム発注側)10人、学生(院・学部)10人で構成。グループディスカッションを通じて、コミュニケーション力醸成と立場の違いを理解する。

受講者の既知識レベルよりも立場の違いを重視して選考。よってレベルは初級、中級、上級と比較的バラバラ。

第三部
評価
(教育訓練システムの評価)

評価の目的は、教育訓練システムを
評価すること

方法論

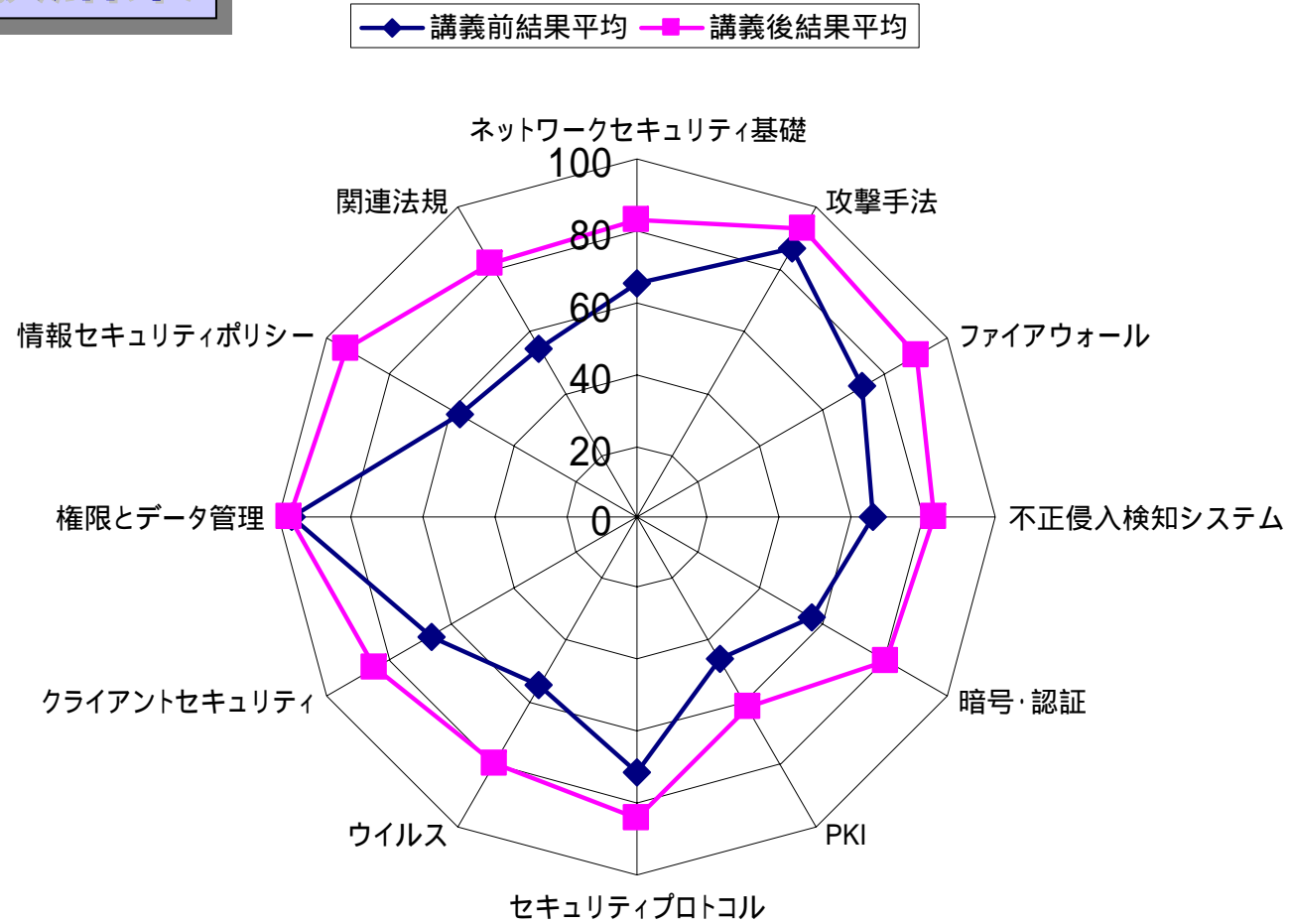
- 1) 受講者能力開発測定(試験及び自己評価)
- 2) 受講者アンケート、ヒアリング
- 3) 講師ヒアリング

- 1) 基礎講座でのスキルチェック試験
受講前、受講後にペーパー試験実施
その差異分析
- 2) アンケートでの自己評価
受講前、受講後、知識面の評価
受講前、受講後、ビジネススキル面の評価
その差異分析

受講者能力測定結果 1



基礎講座試験結果

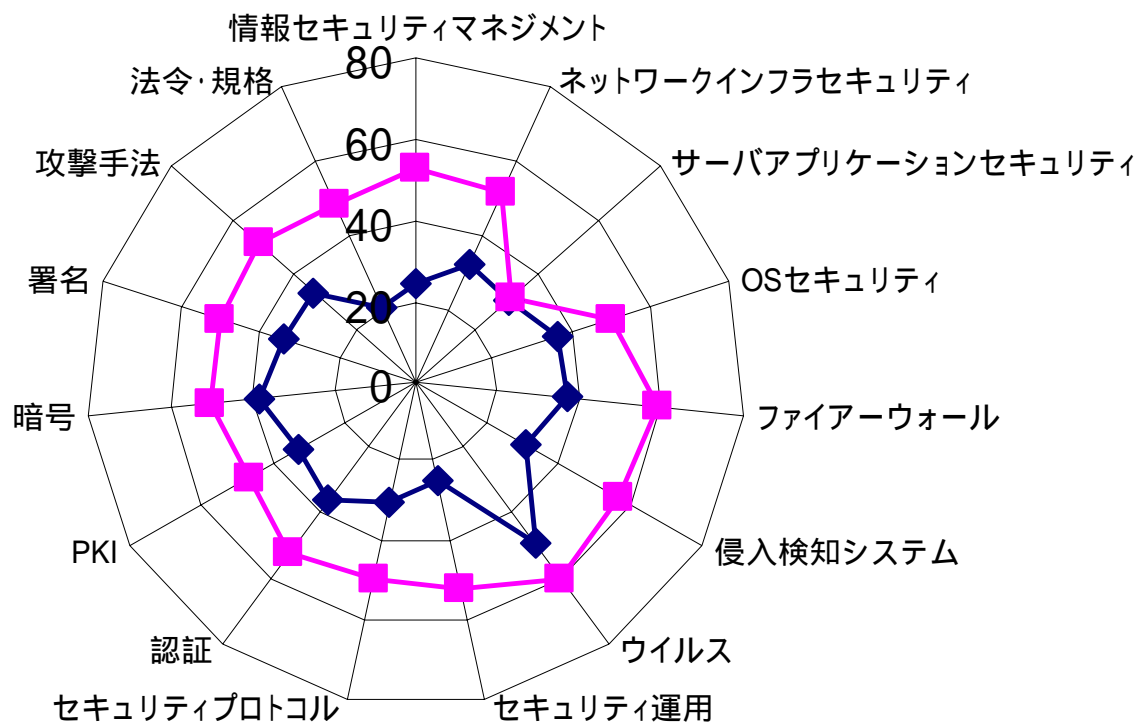


受講者能力測定結果 2



全体評価(知識面)

◆ 受講前合計ポイント ■ 受講後合計ポイント

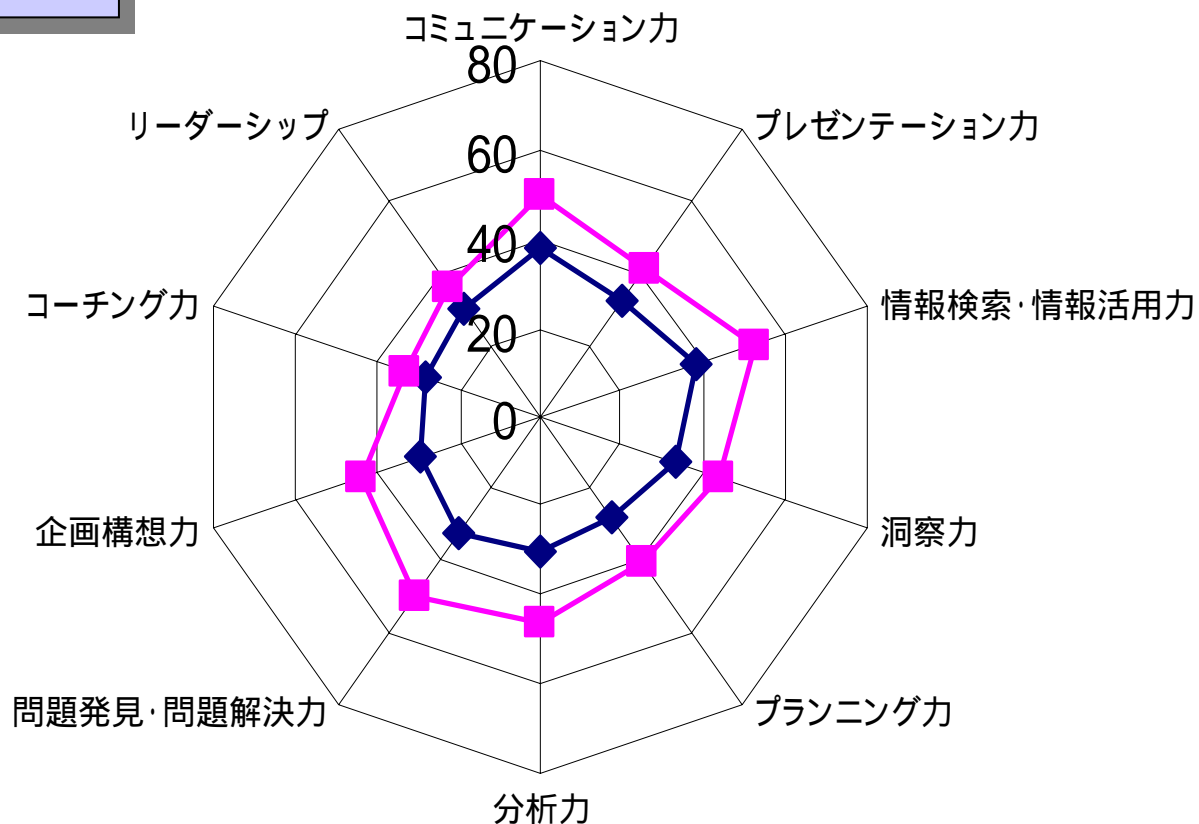


受講者能力測定結果 3



全体評価 (ビジネススキル)

◆ 受講前合計ポイント ■ 受講後合計ポイント

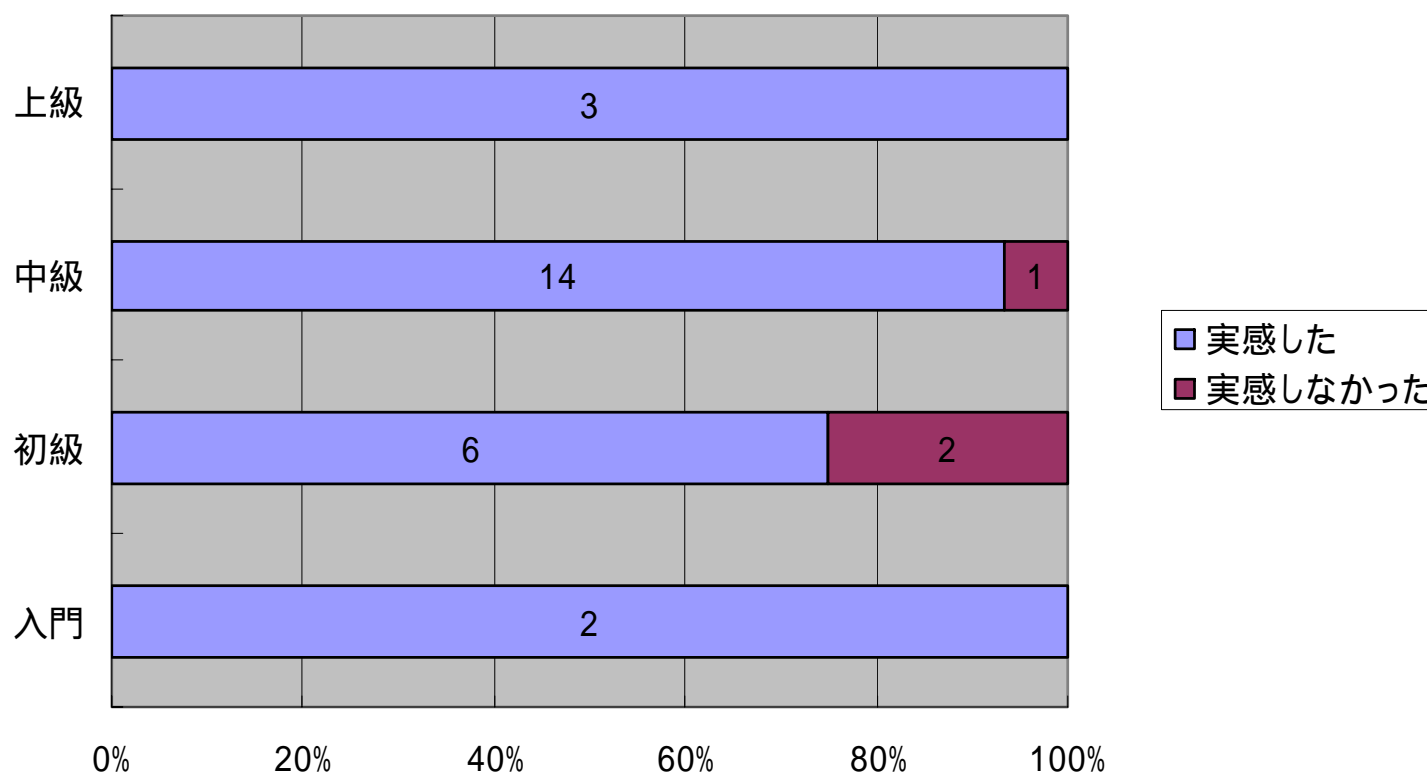


アンケート結果1



包括的理解

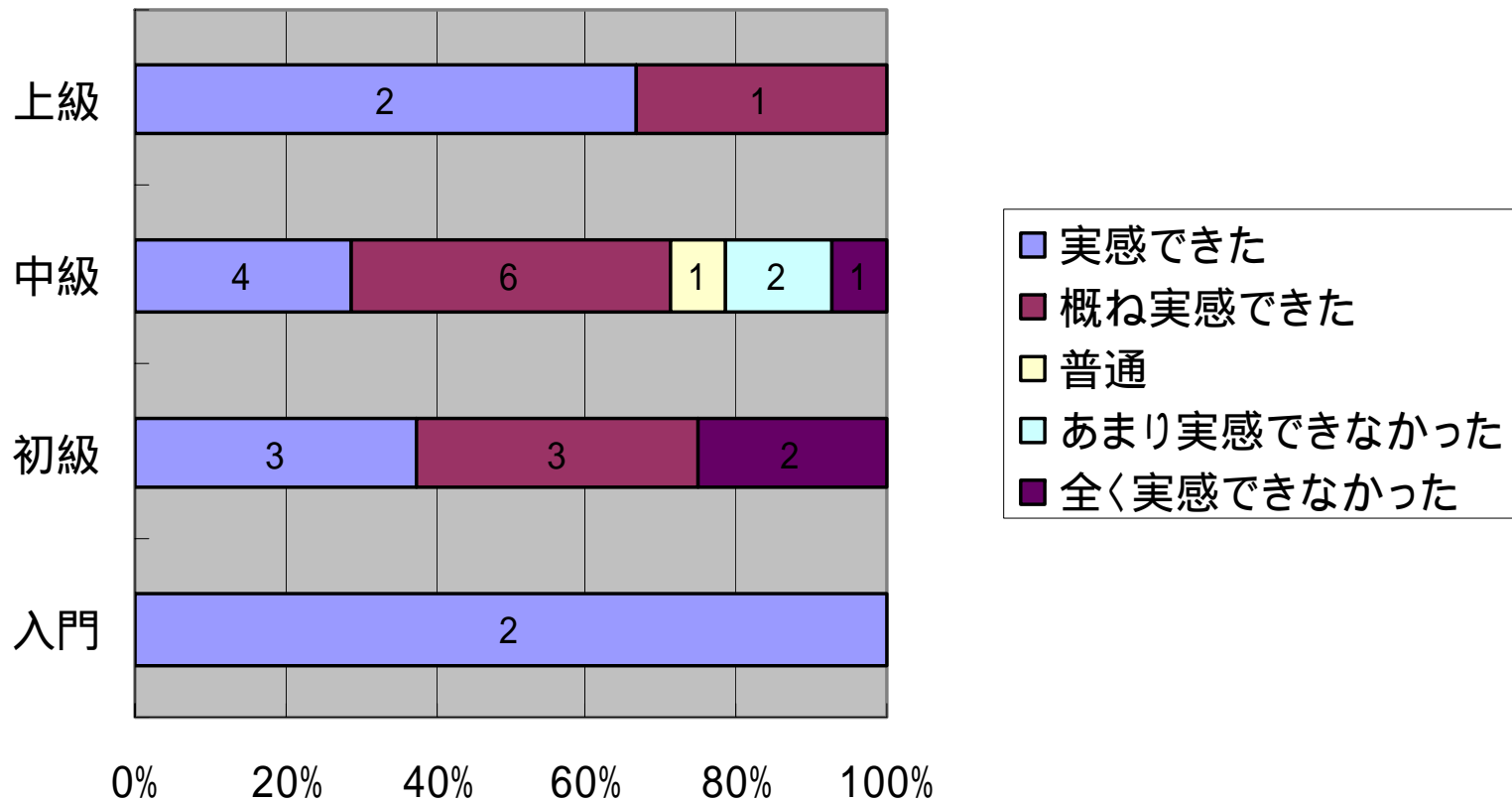
情報セキュリティ分野全体を包括的に理解できたかどうか、その実感について全講座終了後に受講者に伺った。



アンケート結果2



立場の違い、その相互理解



第三部 結論

包括的理解

- 1) 情報セキュリティ分野の全体像を理解させる、又は「プロセス」として捉えられる人材の育成において、ケースメソッドは極めて有効な手法である。
- 2) ケースメソッドは、経営学分野に限定されることなく、情報セキュリティもしくはIT分野でも遜色なく機能する。

立場の違い、その相互理解

受講者から多く聞かれた意見では

「今回のケースでは、問題が明確になっておらず、その分受講者のアイデアが出る余地が大きかったと思う。アイデアを出すという意味では、討論形式の授業が最適と感じた。グループ内から様々なアイデアが飛び出し、物事の捉え方、考え方について非常に勉強になった。」(大学院情報工学研究室T氏)

立場や考え方の違う人同士の討論は、その目的を「相互理解」ではなく、「アイデアを出す」「何か新しいものを生み出す」等の創造的な機能、それらに重点をおいた方が良い。

実験結果3



ビジネススキルの開発

数値面では、ビジネススキル面の向上も一定的には上がっているものの、知識面と比較すると全体的に伸び率は低い。知識獲得より付加価値が高く、その獲得はより難しい。短期間での修得は困難ではあったが、技術的スキル偏重の学生、若手社会人には、知識よりコミュニケーション能力、企画構想力、リーダーシップ等の能力がより重要な要素であることは授業を通じて教授することができた。

- 1) **品質面(ビジネススクールと比較して)**
ビジネススクールのケース教材には、経営における「英知」や「教訓」が多く盛り込まれている。当協会が策定したケース教材には残念ながら情報セキュリティ分野における「教訓」のような要素を組み込むことができなかった。
(そもそも「教訓」とは何であろうか)
- 2) **失敗経験を科学する**
「できるSE」「優秀な技術者」に共通して言えることの一つには、過酷なトラブルを乗り越えてきた経験を誰もが有している。知識やビジネススキル以外に、失敗から学んで得た「嗅覚」のようなものを持ちえているが、今回の実験にはその要素を伝えることができなかった。
- 3) **講師確保**
ケースメソッド式教育は、通常の講義形式の授業と比較し、講師に求められる能力要素が多い。そもそも情報セキュリティ分野全体を包括的に理解している人材が少なく、今後ケースメソッド式教育を展開する障害となるのは間違いない。
- 4) **レベル設定の困難さ**
情報セキュリティ分野は範囲が広く、この分野の専門家(人材像)はスペシャリストではなくゼネラリスト。ゼネラリストであること自体問題ないが、様々なスタンスの取り方が考えられるため、固定的なレベル設定が難しい。

今後の方針



「英知」及び「教訓」の抽出

ケース(事例研究)を通じて、情報セキュリティ分野の「英知」及び「教訓」を抽出すること。

同じ業界、同じような環境下でWeb改竄、個人情報漏洩事件が多発している。

原因の多くは、似たようなものと想定しうるも、「教訓」が体系化されておらず、事件、事故が繰り返されている。

技術的解説書は、多く流通しているも、「教訓」を体系化したものは存在しない。

そこで、本事業の成功及びそこで得たノウハウの利用、及び当協会のフレームワークを生かし、来年度以降ケース(事例研究)を通じた情報セキュリティ分野の「英知」「教訓」を体系化していきたい。

「高度 IT 人材育成システム：ITSS 実証実験」 ケースメソッドによるセキュリティスキルアップ教育

作成者：松田 剛（教育部会：ITSS 実証実験技術評価 WG リーダー、株式会社ヒューコム）

(1) 背景と目的

現在提供されている情報セキュリティ教育は、ファイアーウォールや暗号理論等の個別分野が各々分立し一貫した教育訓練が提供されていない。よって分野横断的かつ体系だった思考のできる人材が極めて少ない。しかし企業等の実務現場で求められているのはその種の人材、つまり分野全体を包括的に理解した人材であり、現場第一線に従事する技術者は情報セキュリティが必要とする膨大な知識の習得が不可欠である。

知識対象の広さの観点より情報セキュリティは「総合科学」的色彩の強い分野と考えられるが、知識として秩序だった体系が存在しないこと、現在提供されているセキュリティ教育が個別分野の知識偏重に限定されていることを特に問題と認識した。

個別分野の専門家では情報セキュリティを一連の「プロセス」として捉えることができず、現行の教育サービスで育成しうる人材と企業の求める人材像の間での乖離が見受けられる。よって本教育訓練事業実施に先立ち、「情報セキュリティ政策のグランドデザインができる人材育成」を事業目的の一つと設定し、以下の 3 つの要素をその達成に必要な不可欠のものとした。

- ・ 個別分野の専門家ではなく、それら分野を横断的に捉えられるスキルを有する人材
- ・ 知識偏重ではなく、知識の組み合わせによる問題解決能力、創造力、分析力、企画構想力、コミュニケーション能力などを能力開発の主眼に置く
- ・ 他分野の職種又は立場の違い、その相互理解

教育訓練の実施及びカリキュラム開発については、ハーバード大学に代表される米国ビジネススクールの教育手法「ケースメソッド」を参照した。金融工学を筆頭に現代経営学は、個別分野の先鋭化が目立つがケースメソッドは個別技術論に特化せず、それらを含めたゼネラル的な視点（つまり経営者の観点）を授与する機能に優れている。当協会は、ケースメソッドの持つこの機能が、情報セキュリティ教育が抱える問題の一解決策になると仮定しこれを採用、本教育訓練事業を通じてその有効性を評価した。

(2) 実施内容：カリキュラム

大きく基礎、応用、ロールプレイングと 3 つの講座に分割した。更に応用講座は、マネジメントコース、技術対策コース、ケースメソッドと各コースに分け、マネジメントコース、技術対策コースは選択制とした。各コースの詳細を表にまとめる。

講座	コース	受講形態	内容	目的
基礎講座		選択制(1)	攻撃手法、暗号、ウイルス等 12 項目	基礎知識習得
応用講座	マネジメント	選択制(2)	リスク分析、ポリシー策定等	実践的知識習得
	技術対策	選択制(2)	盗聴対策、セキュアサーバ構築等	実践的知識習得
	ケースメソッド	受講必須	事例研究を通じた包括的な情報セキュリティ対策学習	情報セキュリティ分野のロジカルシンキング
ロールプレイング		受講必須	ケースメソッドで提示された課題解決の発表会	発表会及び評価

(1)受講は任意、既に基礎知識を有していれば応用講座からの受講可、(2)マネジメント若しくは技術対策どちらかを選択受講

(3) 成果

情報セキュリティを一連のプロセスと捉えさせることが、組織全体のセキュリティレベル維持・向上に不可欠の要素と既述したが、ケースメソッドによりその包括的理解、大局の見地から物事を考える、その視点を教授できたことは評価データに顕著に表れた。

対象範囲が広い当分野は、「基礎から一歩着実に…」式学習あるいは、講師が一方向的に話す形式の授業、暗記中心など伝統的な教育手法では一人前に成長するまで多大な時間を必要とする。伝統的教育と比較すると学習効率性の面からもケースメソッドの評価は優れていた。ケースメソッドは、経営学分野に限定されず IT を含む情報セキュリティ分野でも遜色なく機能し極めて有効な手段と言える。

(4) 課題と今後の展望

ディスカッション主体(受講者同士)のケースメソッド式授業は、一見講師は何もしないような印象をもたれるが、伝統的講義(講師が一方向的に説明を入れる)と比べると講師にかかる負担は比較にならない程重い。講義の場では、受講者からどのような指摘を受けたと的確な答弁、あるいは絶対的なリーダーシップなどの高度な能力が必須である。そもそも情報セキュリティ分野全体を理解している人材が少ない上、更にケースメソッドが求める高度テッチングスキルを有する人材は皆無に等しく、この教える側の人材不足が今後の展開の足かせとなるのは間違いない。

また教材に使用したケース(事例)も実績あるビジネススクールのもの比べると内容、品質面でかなりの格差があり、ケースの中に「英知」や「教訓」をふんだんに盛り込むことができなかった。その格差縮小が今後の課題、当面の目標である。

今後の展望としては当協会の性格上、本式教育を継続的に実施していくことは難しいものの、本教育訓練事業にて得たノウハウを積極的に公開し、主として会員企業(2004年2月現在181社)向けに還元、教える側の育成を通じて本式教育の普及を計る。

製造業、金融業、IT産業、政府機関等業態を問わず情報セキュリティに秀でた人材の輩出は、我が国が強みとしてきた高品質、高信頼性社会の維持、実現に寄与するだけでなく、しいては国際競争力を持った情報セキュリティ産業構築に貢献することとなるであろう。