JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

情報セキュリティ教育実証実験 プロジェクト H17 活動報告

NPO日本ネットワーク
セキュリティ協会
松田 剛

プロジェクトチーム発足の背景

チームの発足

・経済産業省の支援により、17年度にプロジェクトチーム発足

設立の背景

1. 情報セキュリティ教育市場は拡大基調にあるものの、多種多様なカリキュラム が乱立し、全体的に秩序だった発展を遂げているとは言えない。またユーザ企業では大企業と中小企業の間でこうした対策状況に格差が見受けられる。（民間部門）
2. 大学部門では、伝統的に暗号などの理論教育は強いが、ネットワークセキュリティ分野を含む包括的カリキュラムの実践例は少ない。また首都圏の大学と地方大学でその取り組み格差が見受けられる。（大学部門）

民間部門の教育サービス状況

サービス分類（例）

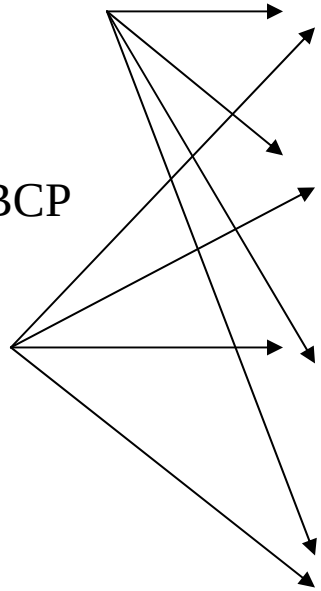
政策系

- 情報セキュリティ；ISMS
- 個人情報保護
- 事業継続管理、危機管理；
  IR、クライシスハンドリングBCP

技術系

- ウイルス対策
- 認証技術、PKI
- OS・サーバセキュリティ
- ファイアーウォール
- 侵入検知
- 暗号、電子署名
- 不正アクセス手法

・・・・etc



受講対象者（ユーザ企業）

経営管理者層

- CIO、CISO、情報セキュリティ委員長、監査役・・・

実施責任者層

- CIO補佐、CIO補佐官、メディアセンター長、情報システム部門長・・・

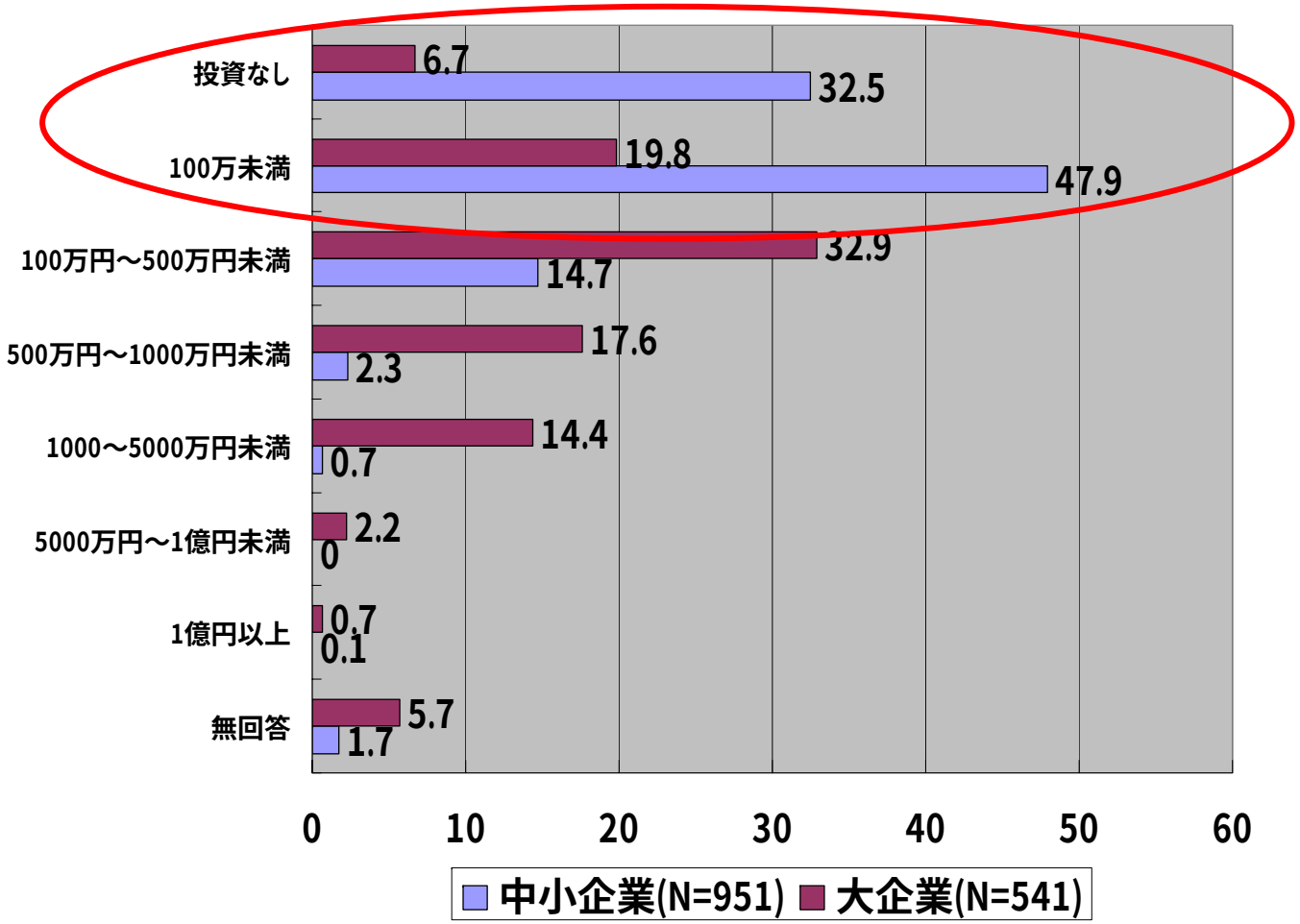
実施担当者層

- メディアセンター職員、情報システム運用担当者・・・

一般利用者層

- 営業部門、経理部門、総務部門・・・などのPC利用者

セキュリティの取組状況 (ユーザ企業)



出典；「情報セキュリティ対策の状況調査」総務省、２００２

大学部門の教育実施状況（1）

- 一部大学では、本格的に専門家育成コースを展開している（例※）
  - 情報セキュリティ大学院大学（横浜）
  - カーネギーメロン大学（兵庫）
  - 工学院大学
  - 中央大学
  - 東京電機大学
- しかし大多数の大学、特に地方大学では精力的に展開しているとは考えにくい

（※）他に、早稲田大学・大阪大学・横浜国立大学・東京大学・慶応義塾大学・筑波大学等が学部レベルを中心に実施している模様（筆者が知る限り）

大学部門の教育実施状況（2）

目的

現代の情報セキュリティ技術には、計算量理論的安全性に基づく技術と、情報理論的安全性に基づく技術がある。その両者について、その代表例を紹介する。本科目は、情報セキュリティの技術的な側面が中心である。社会的な観点から見た情報セキュリティのあり方や課題などについては、別途教える必要がある。

概要

情報セキュリティ技術として最近開発されてきた様々な技術を学ぶ。具体的には、計算量理論的安全性に基づく技術（公開鍵暗号、デジタル署名、零知識証明）と情報理論的安全性に基づく技術（秘密分散共有法、認証コード）について学ぶ。

[修得項目]

情報セキュリティ技術の原理（計算量理論的安全性、情報理論的安全性）、情報セキュリティ技術の使われ方

[知識項目]

鍵共有暗号、公開鍵暗号、デジタル署名、零知識証明、秘密分散共有法、認証コード、暗号の安全性

[関連項目]

情報セキュリティの社会的な意味と課題、情報倫理

講義項目

1．公開鍵暗号への導入[1]

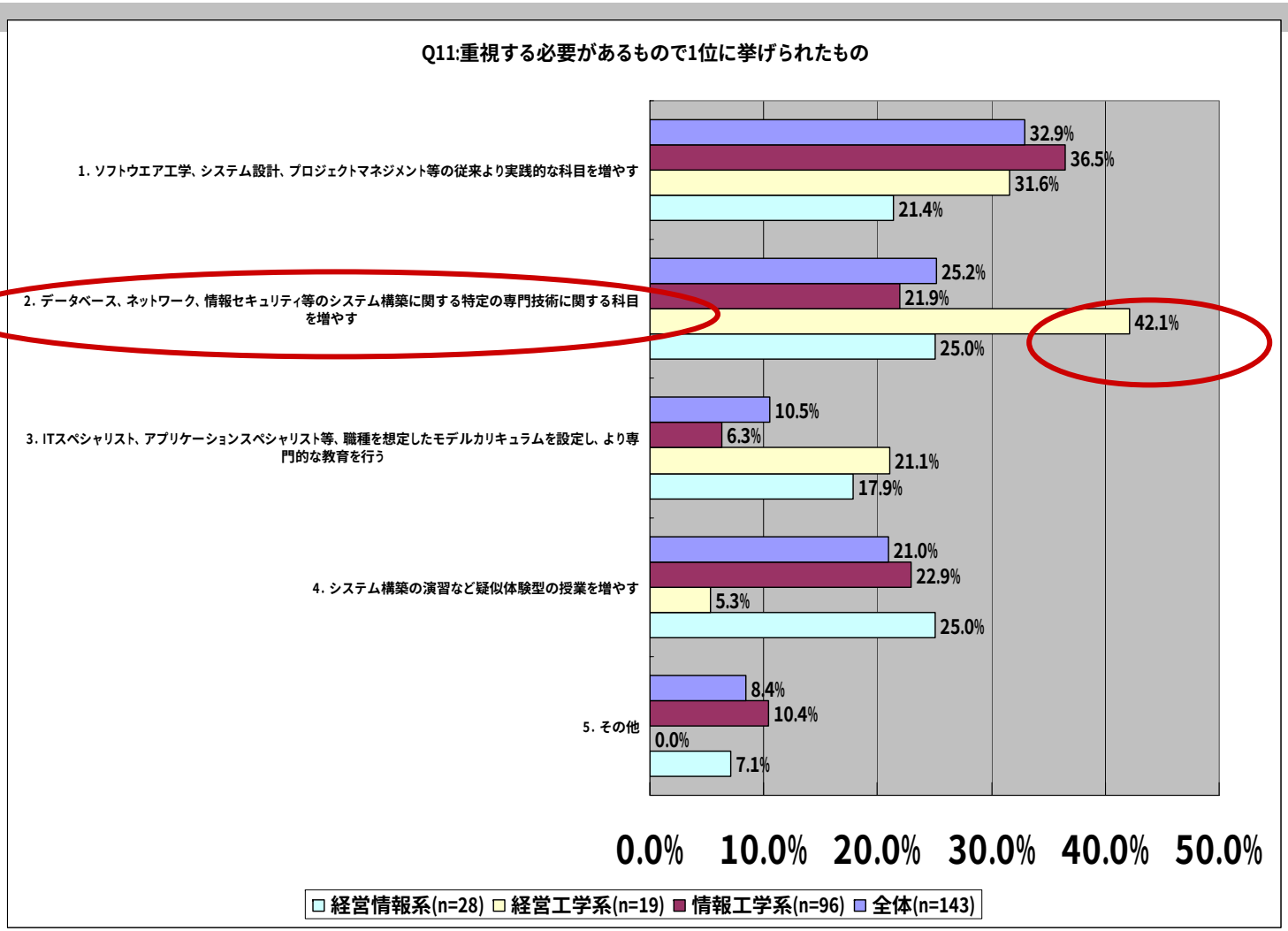
2．RSA暗号[2]

3．零知識証明[3]

・・・中略・・・

（出典；大学の理工系学部情報系学科のためのコンピュータサイエンス教育カリキュラム第1.1版（J97）情報処理学会）

大学部門の教育実施状況（3）



（出典；大学における産学連携情報処理教育の現状に関する調査報告書；経済産業省平成16年）

論点整理（問題意識）

- 情報セキュリティ分野の人材育成で、大学は産業界が求める人材を輩出できているか？
- そもそも産業界はどのような人材を求めているのか、それらを大学に伝えているか？
- 情報セキュリティ分野の教育インフラは社会が求めるものについて十分整備されているのか、教育の機会は全国均一的に提供されているのか（需給バランスは適切か）？
- 多種多様なカリキュラムが乱立するセキュリティ教育マーケットは、この状態のままで良いのか？
- 教育サービス提供側と受講者側でミスマッチは発生していないか？
- 大企業と中小企業、首都圏大学と地方大学の格差の原因は何か。このままの状態が望ましいのか？

活動の目的

活動目的

1. 産学連携によるカリキュラムの構築と講義の展開（大学が得意とする理論分野と企業が得意とする実践例を組み合わせたもの）
2. セキュリティ教育に係わる普及啓発活動
3. 人材育成に携わる現場の調査

活動内容

1. 東京電機大学（通年）、工学院大学（2005.12）、岡山理科大学（2005.12）の協力により講義を展開
2. 岡山県（2005.12）、東京（2006.3）「情報セキュリティ人材育成シンポジウム」の開催
3. 教育現場（大学、産業界）の実態調査

実績の報告（1）

（東京電機大学の講義実施要領）

講座名 ： 「暗号とその応用」
担 当 ： 佐々木良一教授
開講日時； 2005年4月13日（水）～7月13日（水）17:30～19:00（毎週水曜日、前期）
概 要 ： セキュリティ技術の基礎となるが社会人がしっかり学ぶ機会がない暗号技術について、（1）基本の部分から、（2）デジタル署名などの応用技術、（3）電子商取引や電子政府における利用方法などについて体系的に教育する。

講座名 ： 「ネットワークのセキュリティ」
担 当 ： SEA/J 講師（伊藤栄二氏）
開講日時： 2005年4月13日（水）～7月13日（水）19:10～20:40（毎週水曜日、前期）
概 要 ： 公開サーバとそれを取り巻く境界（ペリメータ）ネットワークでのセキュリティ対策を解説する。実践で使える対策技術を効率よく学ぶため、講義とは別に、学んだ知識（理論）を実証する場として実際に公開サーバ（DNS、メール、Web）を構築、運用するワークを受講生が行う。またファイアウォール、IDSの導入から境界でのセキュリティ対策を理解する。

講座名 ： 「不正侵入対策の実際」
担 当 ： SEA/J 講師（伊藤栄二氏）
開講日時： 2005年9月14日（水）～2005.1/11（水）19:10～20:40（毎週水曜日、後期）
概 要 ： 前期が事前（プレ）の対策とするならば、後期では事件（インシデント）発生を前提とした事後対応（インシデントレスポンス）技術を解説する。前期構築した公開サーバ環境の運用を行いながら不正侵入対策に的を絞り、主にIDS のチューニング、ログ解析からインシデントレスポンスの技術を学ぶ。

（※） 岡山理科大学、工学院大学の実施要領は付録に掲載

実績の報告（2）

人材育成シンポジウムの開催（岡山）

標　題　：　情報セキュリティ人材育成シンポジウム in 岡山
開催日時：　2005年12月16日（金）13:30～17:00
開催場所：　岡山市デジタルミュージアム　5階講義室
定　員　：　80名
料　金　：　無　料
プログラム：
講演1「セキュリティ教育の実践と課題　～東京電機大学の場合～」
　（講師：東京電機大学工学部情報メディア学科教授　佐々木良一氏）
講演2「セキュリティ教育（リテラシー）は何故必要か」
　（講師：株式会社エス・シー・ラボネットワーク・セキュリティ事業部ゼネラル・マネージャー 木村聡氏）
講演3「NECにおけるIT技術者の育成モデルとセキュリティ技術者育成の取組み」
　（講師：ＮＥＣラーニング株式会社取締役執行役員　山脇英生氏）
講演4「CyberCampusと教育の産学官連携」
　（講師：岡山理科大学総合情報学部情報科学科教授／情報処理センター所長　大西荘一氏）

実績の報告（3）

人材育成シンポジウムの開催（東京）

標　題　：　情報セキュリティ人材育成シンポジウム in 東京（2006年3月）
　　－情報システムの安全を支える中核技術者に期待されること－
開催日時：　2006年3月2日（木）13:30～17:30
開催場所：　工学院大学
定　員　：　１００名
料　金　：　無料
プログラム：
講演1「セキュリティ教育の実践と課題　～東京電機大学の場合～」
　（講師：東京電機大学工学部情報メディア学科教授　佐々木良一氏）
講演2「企業および大学でのセキュリティ教育の経験から」
　（講師：株式会社情報数理研究所　専務取締役　伏見 諭氏）
講演3「課題解決型学習を中心とした工学院大学の取組」
　（講師：工学院大学CPDセンター教授　小野 諭氏）
パネルディスカッション「期待される人材像と教育方法と評価方法への提言と議論」
モデレータ：工学院大学CPDセンター教授　小野 諭氏
パネラー：　東京電機大学工学部情報メディア学科　教授　佐々木 良一 氏
　　株式会社ディアイティ　マネジャー　河野 省二 氏
　　株式会社ヒューコム　代表取締役社長　井上陽一 氏
　　株式会社情報数理研究所　専務取締役　伏見 諭 氏

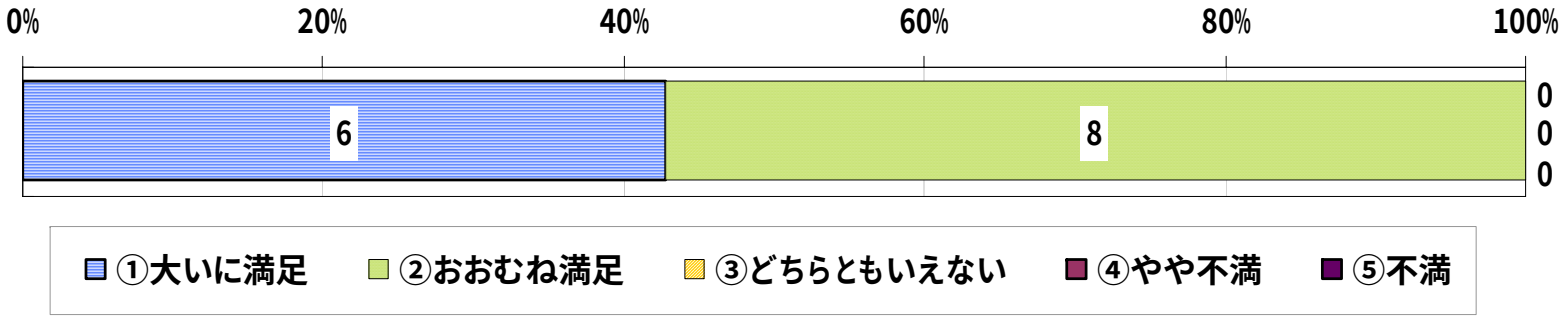
実績の報告（4）

情報セキュリティ教育の現状に関する調査

- 有識者へのヒアリング調査（大学側）
  情報セキュリティ大学院大学　辻井重男学長
  東海大学　菊池浩明助教授
- 情報セキュリティ教育への参加に関するアンケート調査
  （産業界側）
  教育参加が期待されている産業界側の専門家としてJNSA会員向けにWebアンケート調査を実施

教育実績の評価

(工学院大学での受講者評価)

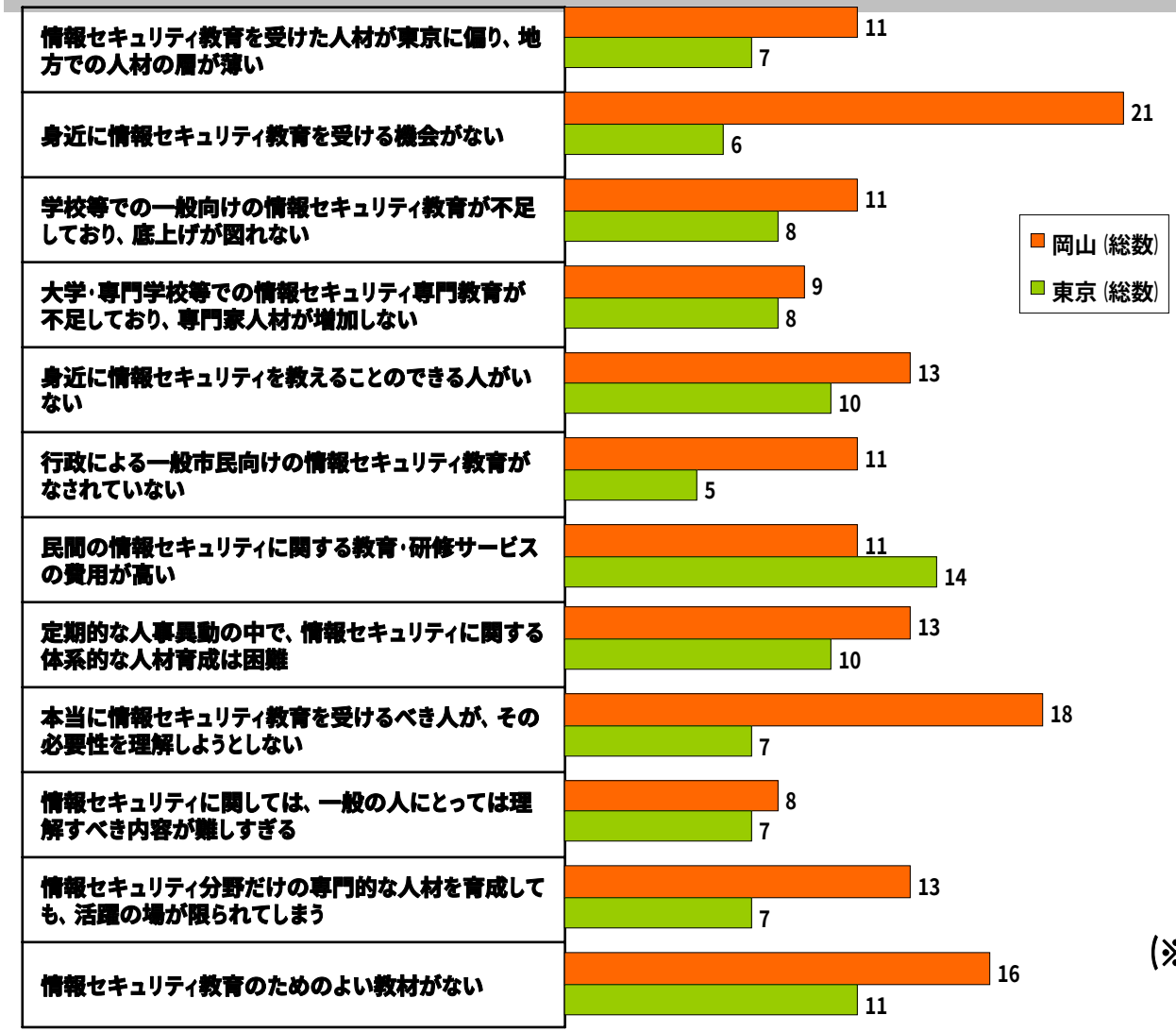


(受講者の声)

- 実習が多くて良かった。分かりやすかった
- 実践と知識をつなげた講座の内容はよかった
- 知識・技術と実例を体験できる講義が理想

(※) 工学院大学での実施は、「セキュアシステム設計技術者の育成」と題したCPD (Continuing Professional Development) センターで、特別講義として実施した。受講者は社会人が中心

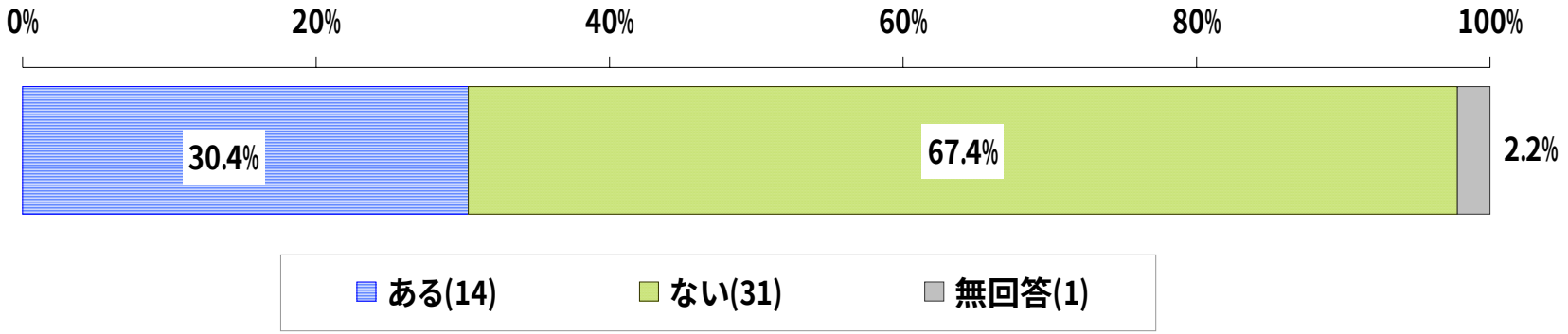
シンポジウム実施結果の考察



（※） 岡山、東京の人材育成シンポジウム参加者アンケート結果より

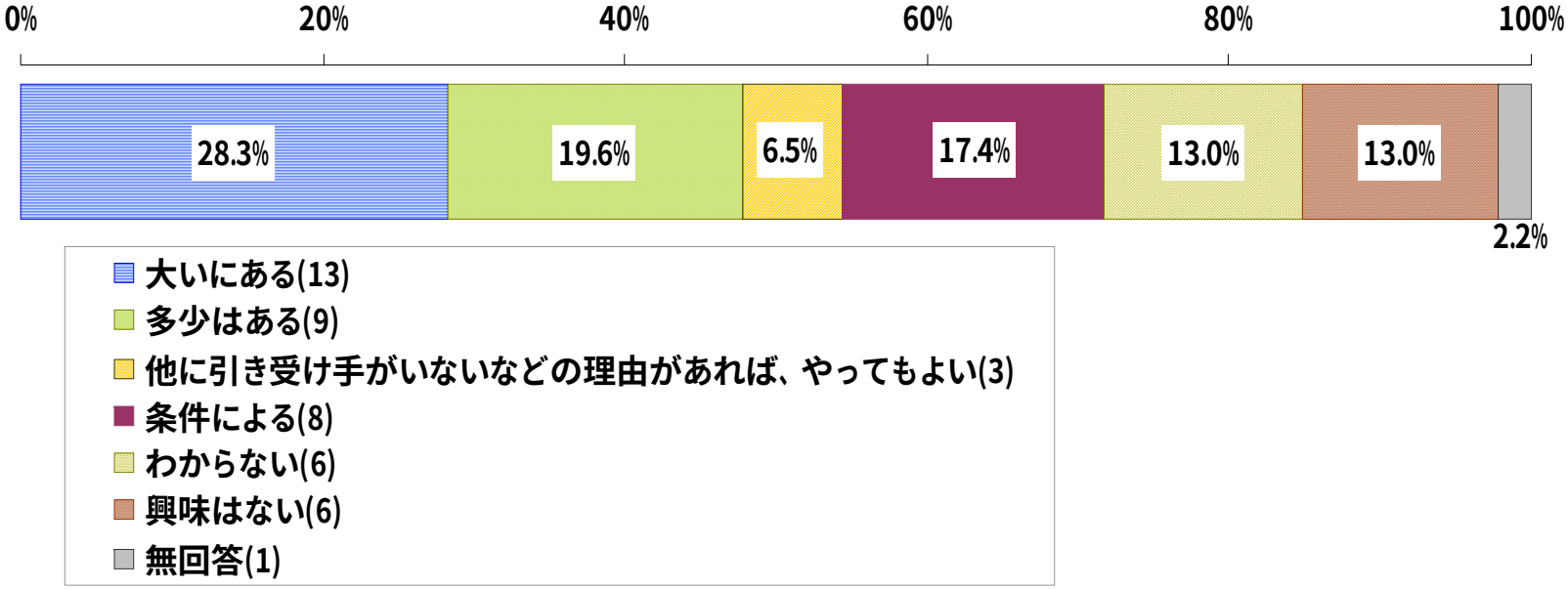
調査結果の考察（1） -産業界-

（産業界の専門家（JNSA会員）向け調査：セキュリティ教育への参加に関するアンケート結果より）



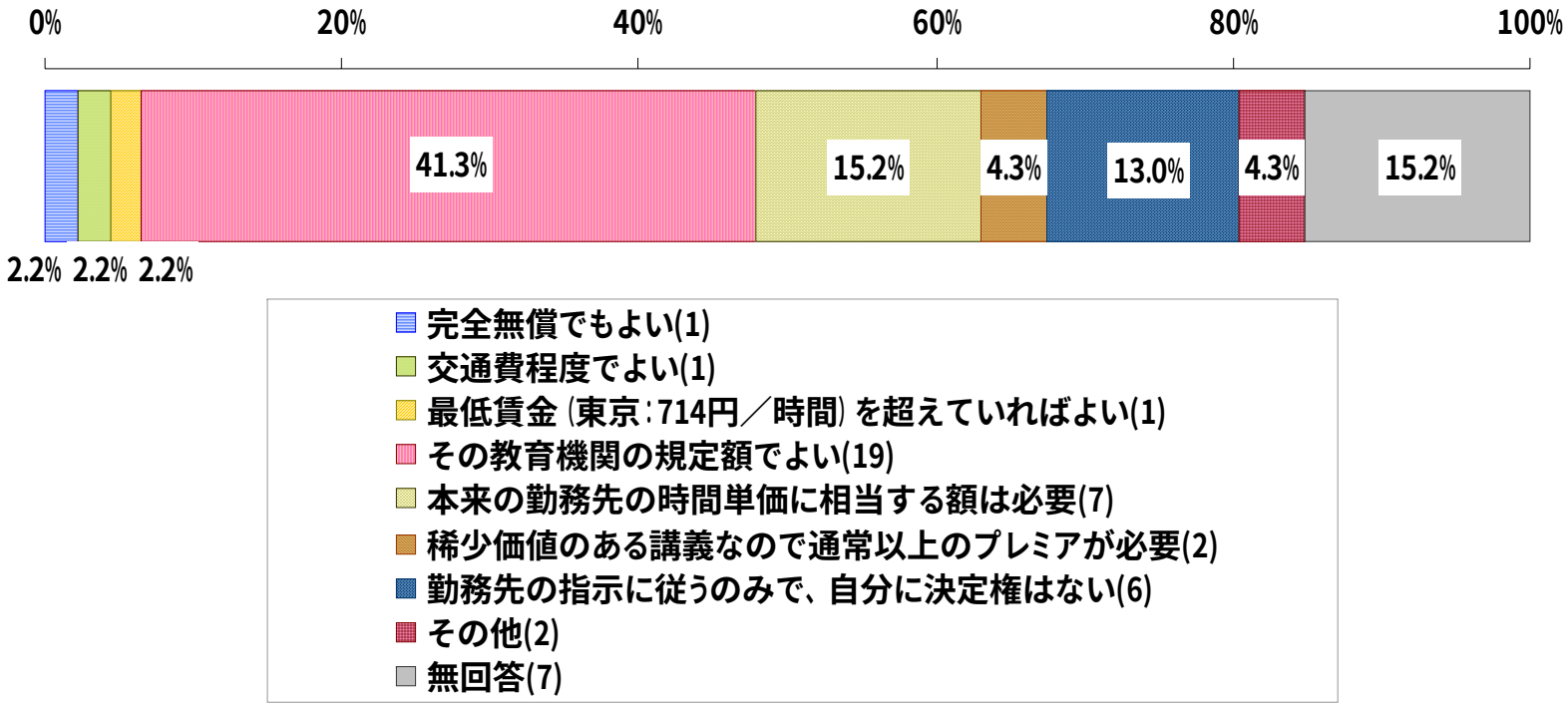
- 講師経験の有無 ： 本来の業務とは別に、大学や専門学校等、公的施設等で情報セキュリティ関連（情報倫理等を含む）の講師を行った経験（n=46）

調査結果の考察（2） -産業界-



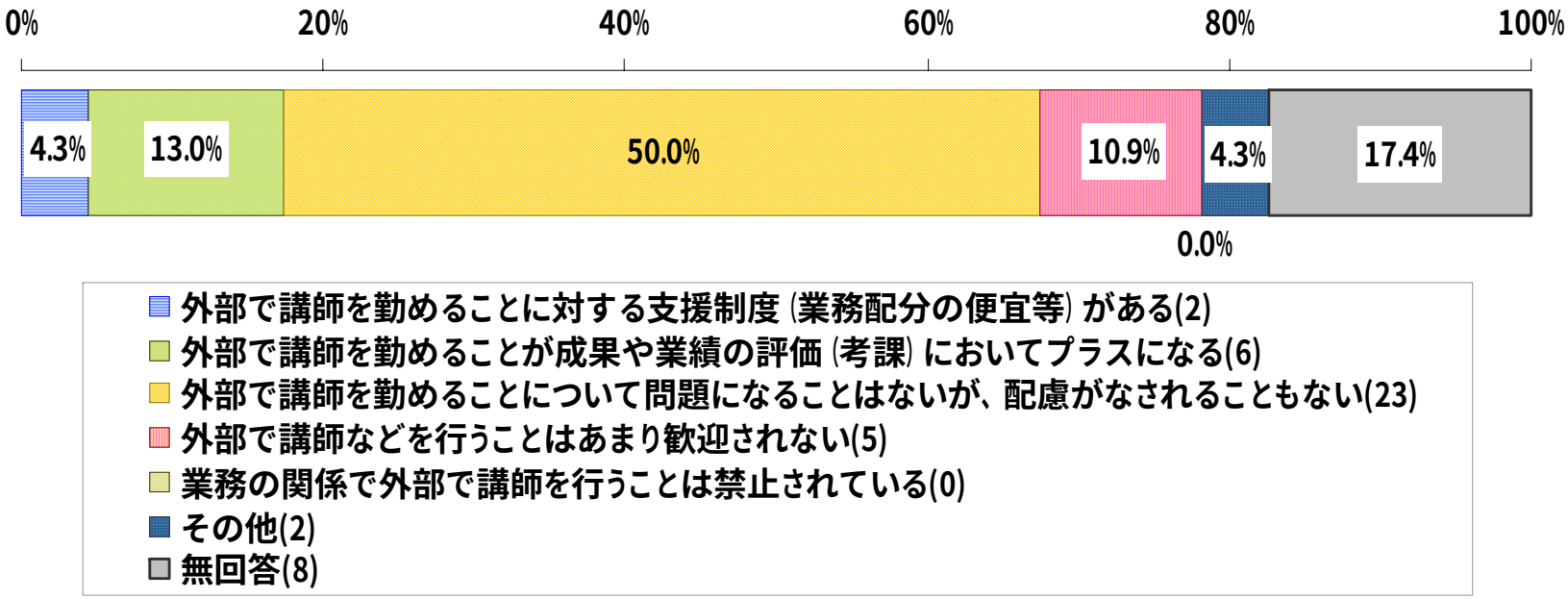
- （産業界の専門家として）大学や専門学校等で情報セキュリティ関連の講義を勤めることへの興味（n=46）

調査結果の考察（3） -産業界-



- **講師報酬の希望・条件**（n=46）

調査結果の考察（4） -産業界-



- **外部で講師を勤めることに関する（勤務先の）支援もしくは制約**（n=46）

調査結果の考察 -有識者-

(ヒアリング調査結果:辻井学長、菊池助教授)

- 地方と東京の情報格差は必ず出てくるところ。セキュリティでは特にそういう差が出る
- 研究系と実務・実践系の切り分けはどうしても生じてしまう。暗号理論で数学の応用を研究している人がフィッシング対策をやるといっても違う・・・(略)
- 企業から複数の講師を呼ぶような場合の事前のアレンジメントは自分がやるよりも大変である。評価はさらに難しい。テストやレポート、採点まで忙しい講師にお願いできない・・・(略)
- ・・・非常勤講師になる資格を持った人にお願いできれば理想的であるが、難しい。博士の学位が必要・・・実際には教えるべき人が学位をもっていないことが多く、大学側で受け皿を用意する覚悟が必要だが、プライドの面で消極的な教員もいる

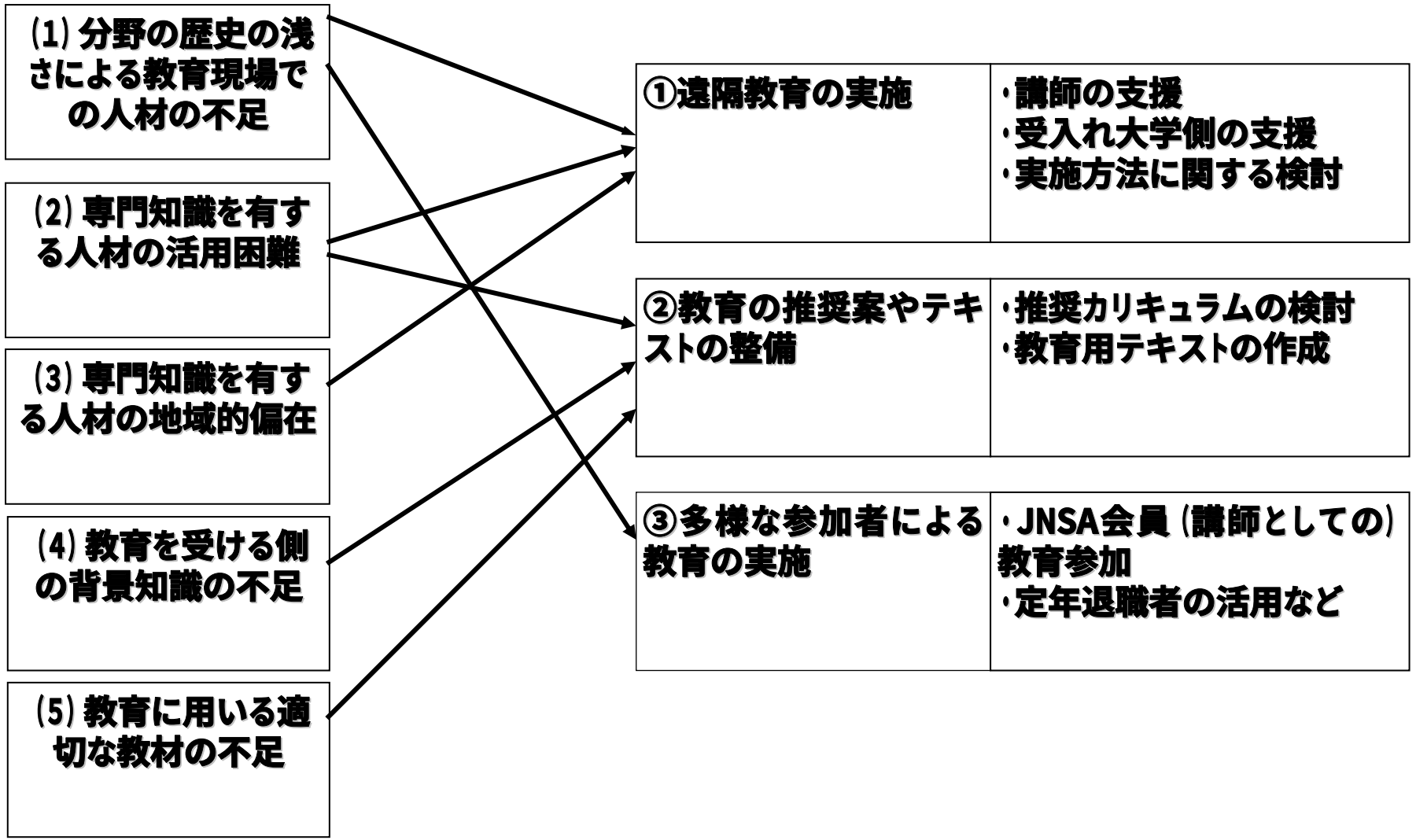
まとめと今後に向けた課題の整理

JNSA

(産学連携式教育、その普及にあたっての阻害要因)

1. 分野の歴史の浅さによる教育現場での人材の不足
2. 専門知識を有する人材の活用困難
3. 専門知識を有する人材の地域的偏在
4. 教育をうける側の背景知識の不足
5. 教育に用いる適切な教材や機材等の不足

H18　実施計画の概要



付録：カリキュラム（1） -東京電機大学講義1-

講義日程	タイトル	内容
第一回	イントロダクション	最近のネットワークの動向を示すとともに、セキュリティの脅威としてどのようなものがあるか、攻撃方法の概要について解説する。
第二回	セキュリティ技術と暗号技術の概要	セキュリティへの脅威に対処するための対策技術を広く概説するとともに、暗号技術の概要を述べる。
第三回	共通鍵暗号1	共通鍵暗号としてストリーム暗号とブロック暗号があることを示すとともに、ブロック暗号の代表であるDESの具体的処理方法を解説する。
第四回	共通鍵暗号2	共通鍵暗号の適用モード、解読方法、鍵管理などについてその方法を解説する。
第五回	公開鍵暗号1	公開鍵暗号のニーズと方法の概要を述べるとともに、RSA暗号の具体的方法を述べた後、演習を行い実際に暗号復号を行う。
第六回	公開鍵暗号2	公開鍵暗号として、エルガマル暗号、楕円曲線暗号などを解説するとともに、利用形態、攻撃方法について概説する。
第七回	デジタル署名	公開鍵暗号の主要な利用方法であるデジタル署名の方法について解説するとともに、そこで用いるハッシュ関数について説明する。
第八回	PKI1	デジタル署名を運用する上での基盤となるPKI（Public Key Infrastructure）について基本的枠組みを解説する。
第九回	PKI2	PKIの相互認証方法や、公開鍵証明書の無効化の手順を比較評価するとともに、今後の展開のために必要な事項を示す。
第十回	暗号プロトコル	暗号をベースとした秘密分散法や、マルティパーティプロトコル、グループ署名、多重署名等の方法について解説する。
第十一回	不正コピーの防止技術	技術の概要、電子透かしなど
第十二回	全体まとめ	以上で学んだことを要約しつつ、振り返るとともに、標準化の動向や暗号技術が社会に与えた影響などについて議論する。

付録：カリキュラム（2） -東京電機大学講義2-

講義日程	タイトル	内容
第一回	オリエンテーション	講義のオリエンテーション、学習目標の確認
第二回	脅威の理解（1）	能動的攻撃を中心に説明（偵察行為、侵入）
第三回	脅威の理解（2）	受動的攻撃を中心に説明
第四回	脅威の理解（3）	受動的攻撃を中心に説明（特にウイルス、クロスサイトスクリプティング等を説明）
第五回	OSの要塞化（1）	公開サーバとしてWindowsを利用する場合の要塞化ポイントを説明
第六回	OSの要塞化（2）	公開サーバとしてUnixを利用する場合の要塞化ポイントを説明
第七回	OSの要塞化（3）	
第八回	インターネットサーバセキュリティ（DNS）（1）	公開サーバとしての、DNSサーバへのセキュリティ対策を説明、主に脅威の説明と公開サーバの構築実習
第九回	インターネットサーバセキュリティ（DNS）（2）	
第十回	インターネットサーバセキュリティ（メール）（1）	公開サーバとしての、メールサーバへのセキュリティ対策を説明、主に脅威の説明と公開サーバの構築実習
第十一回	インターネットサーバセキュリティ（メール）（2）	
第十二回	全体まとめ	前期講義のまとめと、試験実施

付録：カリキュラム（3） -東京電機大学講義3-

講義日程	タイトル	内容
第一回	オリエンテーション	講義のオリエンテーション、学習目標の確認
第二回	インターネットサーバセキュリティ（Web）（1）	公開サーバとしての、Webサーバへのセキュリティ対策を説明。主にWebサービス全般の脅威と公開サーバの構築実習
第三回	インターネットサーバセキュリティ（Web）（2）	
第四回	インターネットサーバセキュリティ（Web）（3）	
第五回	外部公開サーバ環境へのネットワークセキュリティ対策（1）	（タイトルのとおり）
第六回	外部公開サーバ環境へのネットワークセキュリティ対策（2）	Webサーバへのセキュリティ対策、個人情報漏えいに見るWebサイトの設計、ゲートウエイ、ペリメターでのセキュリティ設計、セキュアなサイト設計のまとめ
第七回	IDSによる侵入検知（1）	不正侵入検知システムに関する概要、動作原理を説明
第八回	IDSによる侵入検知（2）	公開サーバ環境において不正侵入検知システムの構築実習。主にNIDSと公開サーバ構築実習
第九回	インシデントレスポンス（1）	公開サーバ環境でのインシデントレスポンス業務の理解とシステムの構築実習。主にインテグリティチェックシステムと公開サーバ構築実習
第十回	インシデントレスポンス（2）	公開サーバ環境でのインシデントレスポンス業務の理解とログ解析手法の理解。主に証拠保全と解析技術、公開サーバの構築実習
第十一回	セキュリティマネジメント関連法規	マネジメントシステムへの技術対策実装の理解と関連法規の説明
第十二回	全体まとめ	後期講義のまとめと、試験実施

付録：カリキュラム　-工学院大学（CPD）-

日時		時限	概要	詳細
12月3日（土）	10:00〜11:00	1限	脅威と対策を考える（60分程度）	1)脅威の洗出し（机上演習） 2)脅威の説明（講師デモ、机上演習） 能動的攻撃、受動的攻撃 3)対策の洗出し（机上演習）
	11:00〜11:30		DNSサーバセキュリティ bind(Linux) （150分程度）	1)DNSサーバの概要（講義） 2)DNSサーバの構築（実機演習） 3)DNSサーバ（サービス）への脅威 4)DNSサーバ（サービス）へのセキュリティ対策（ゾーン転送対策、キャッシュポイズニング対策）
	11:40〜13:10	2限		
	13:10〜14:00	昼食		
	14:00〜14:30	3限	DNSサーバセキュリティ （続き）	
	14:30〜15:30		メールサーバセキュリティ sendmail(Linux) （150分程度）	1)メールサービスの概要（講義） 2)メールサーバの構築（実機演習） 3)メールサーバへの脅威（講義） 4)メールサーバへのセキュリティ対策（不正中継の対策）
	15:40〜17:10	4限		
12月17日（土）	10:00〜11:30	1限	Webサーバセキュリティ apache(Linux) （180分程度）	1)Webサービス概要（講義） 2)Webサーバの構築（実機演習） 3)Webサーバへの脅威（講義） 4)Webサーバ（サービス）へのセキュリティ対策（コンテンツ配置によるセキュリティ対策、不要な機能の削除）
	11:40〜13:10	2限		
	13:10〜14:00	昼食		
	14:00〜15:30	3限	ペリメターセキュリティ設計 （180分程度）	1)各種サーバの配置を考える（演習） 2)要求仕様からセキュリティサーバ設計を考える（演習）
	15:40〜17:10	4限		

付録：カリキュラム　-岡山理科大学-

講義	タイトル	内容
暗号とその応用入門	情報セキュリティ入門	インターネット社会の安全を脅かすもの（被害事例と被害額、セキュリティ関連用語、脅威の分類）
		ウイルスの侵入と感染・発病の関係（ウイルスの種類、最近の動向、Nimda）
		Malwareとして扱うもの（BOTNET、スパイウェア、キーロガー、Phishing、Pharming）
		ユーザ認証技術（知識を利用、持ち物を利用、身体的特徴を利用、強度評価試験）
		不正侵入方法等 （ソーシャルエンジニアリング、TCP SYN Flood、DOS攻撃、Land攻撃、対策）
	暗号入門	暗号の歴史 （共通化議案号と公開鍵暗号、公開鍵暗号による暗号化のイメージ、総当り法、DES）
		現代暗号の基礎 （共通化議案号と公開鍵暗号、公開鍵暗号による暗号化のイメージ、総当り法、DES、RSA）
		現代暗号の応用 （デジタル署名技術のニーズ、用語（電子印鑑/捺印/印影）、ハッシュ関数、認証局）
		実用化されている暗号（SSL、S/MIME）
	更に知りたい人のために	学会、参考文献

付録：カリキュラム -岡山理科大学-

講義	タイトル	内容
ネットワークセキュリティ	最近のインターネットセキュリティ事件とその背景	個人情報漏えい事件（事例紹介、原因、傾向）
		Phishing（フィッシング）詐欺 （名前の由来、HTMLメール、URL偽装、日本語の例のデモ、対策）
		スパムメール（背景、アドレス収集の手口、対策）
		ウイルス、スパイウェア、bot （ウイルスの例、ウイルスとスパイウェアの違い、bot感染経路、最近の傾向、対策）
		P2P事情と著作権（P2Pとは、日本の現状、WinMXとWinny、関連の話題）
		クロスサイトスクリプティング（掲示板の例）
		脅威の分類（能動的攻撃、受動的攻撃）
	Windowsセキュリティ	Windowsの脆弱性 （脆弱性事例、主要脆弱性、脆弱性の推移と傾向、Webの改ざん状況、パスワードの問題）
		WindowsXP SP2のセキュリティ対策 （強化の内容、セキュリティセンター、ファイアウォール、ポップアップブロック、等）
		Windowsセキュリティ対策 （Microsoft Management Console、セキュリティポリシー、パッチ適用、WindowsUpdate、等）