情報セキュリティ教育の動向とJNSA

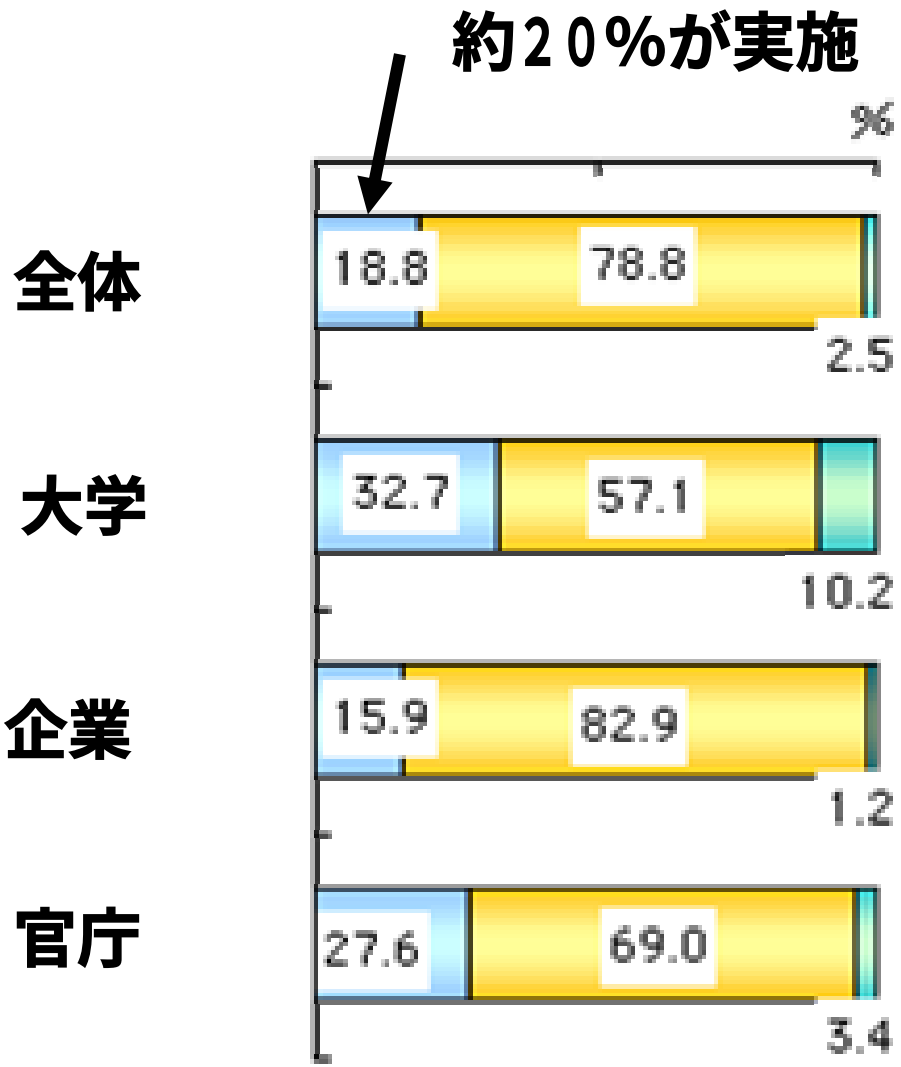
東京電機大学工学部

佐々木良一

sasaki@im.dendai.ac.jp

セキュリティ教育の一般動向

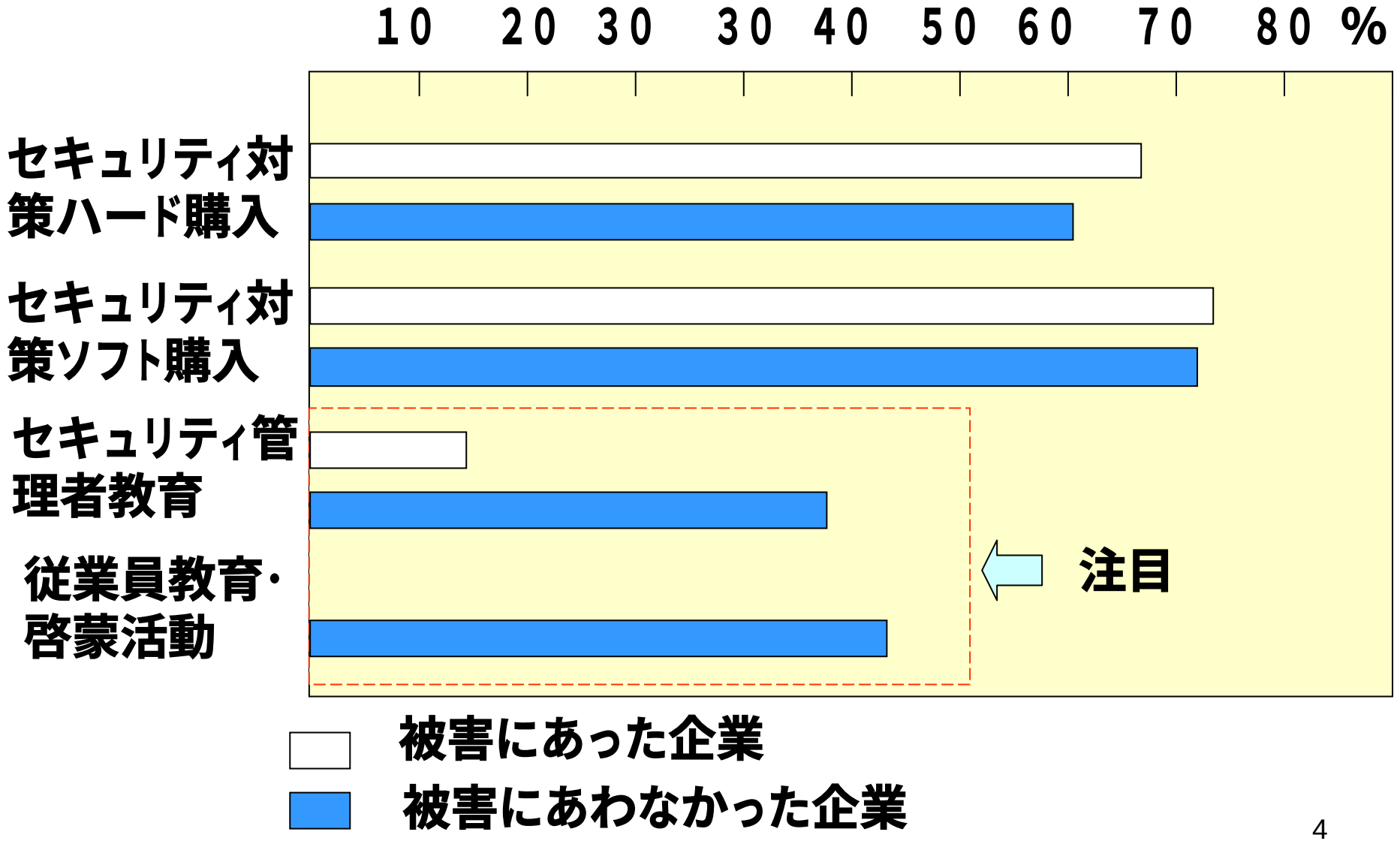
セキュリティ教育の状況



報告書：不正アクセス対策に関するアンケート報告書（2001年6月）

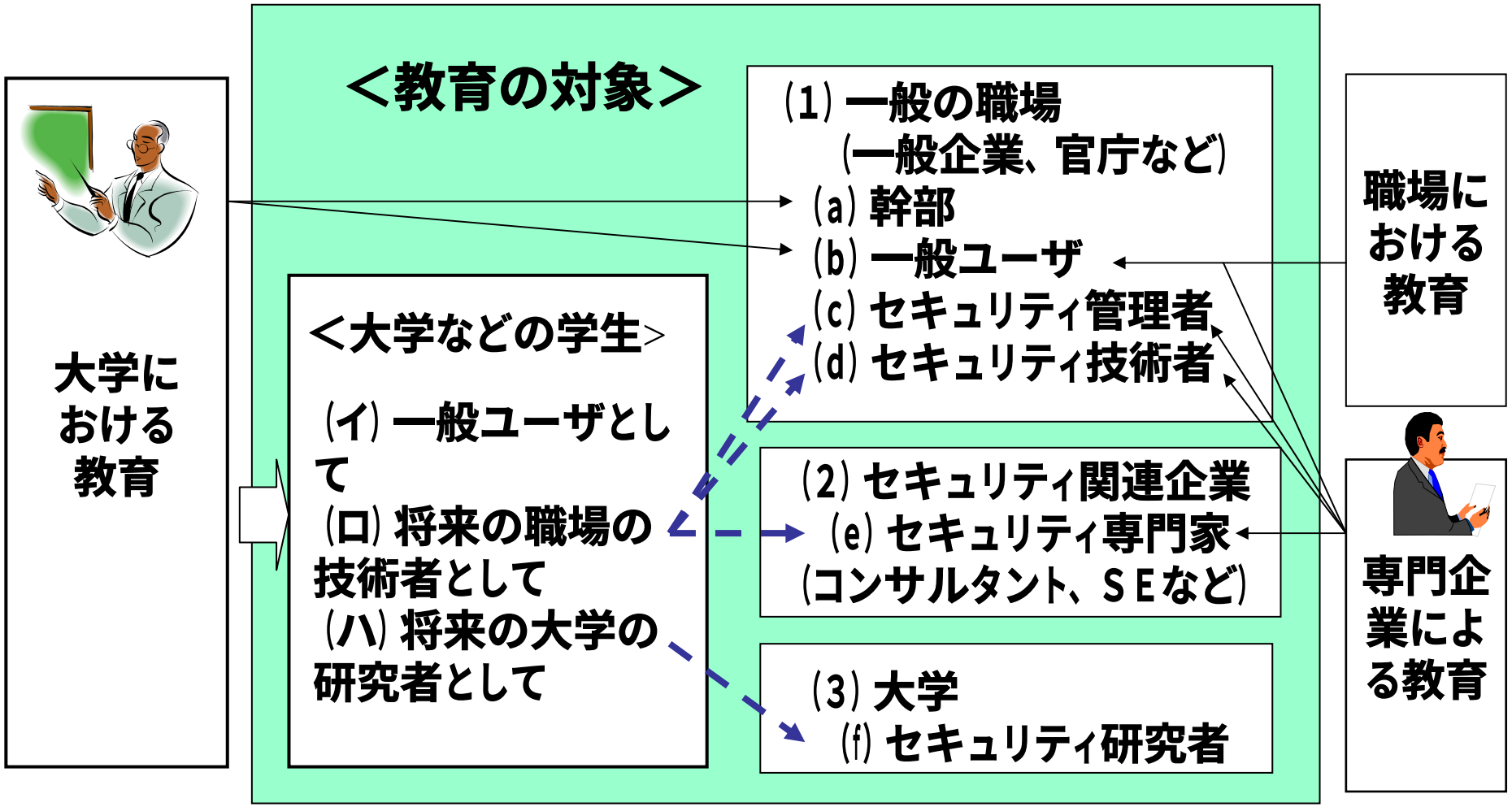
大学が企業に比べ多いがそれでも不十分

セキュリティ教育の必要性



「情報セキュリティインシデントに関する調査報告書2002年度」ＪＮＳＡより

セキュリティ教育の対象



セキュリティ教育のスタイル

技術
レベル

高

低

通常の講義形式

実習・実技形式

ケーススタディ形式

教材やインターネットを用いた自習形式

オンザジョブトレーニング

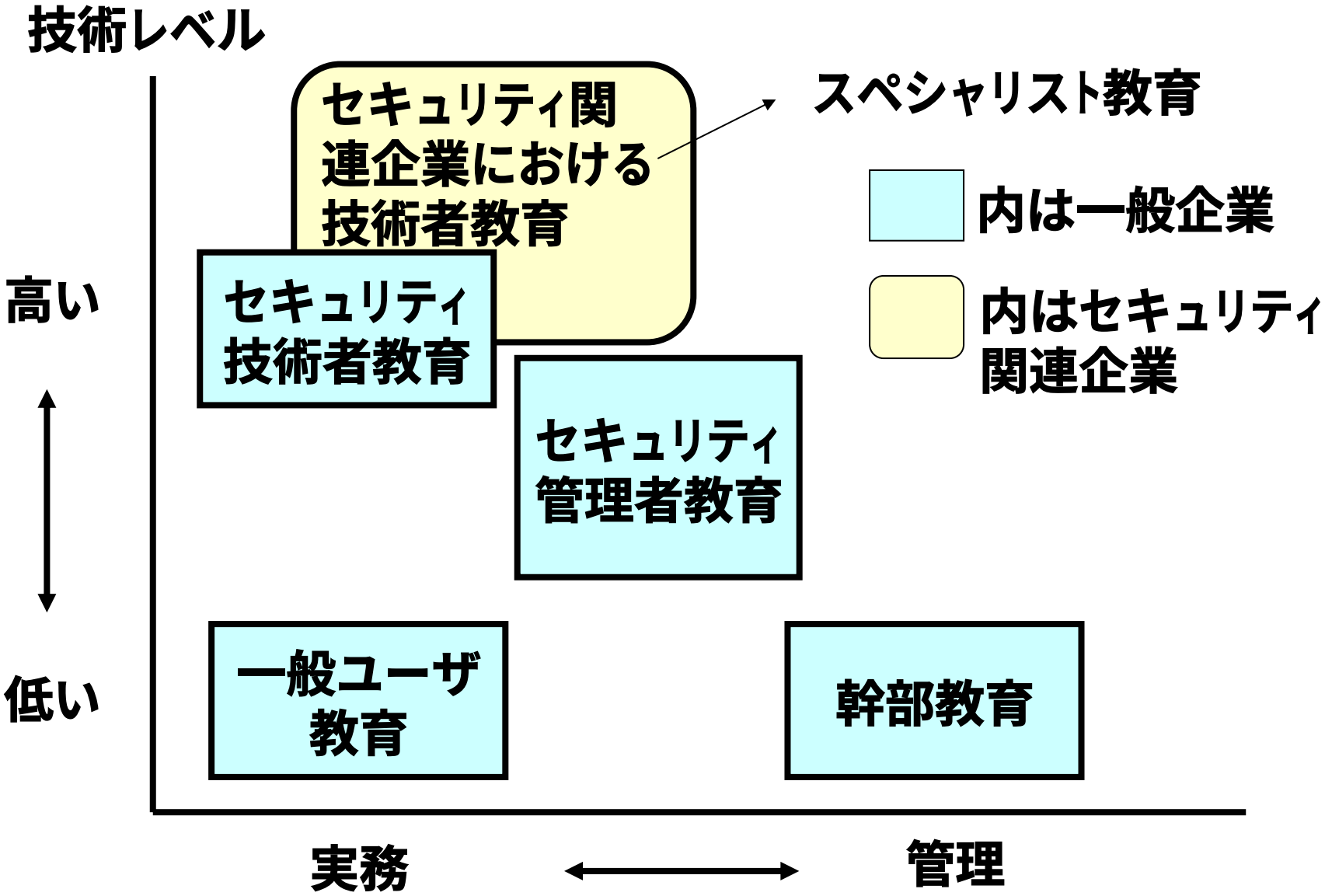


図　各種セキュリティ教育の位置づけ

セキュリティ専門家の分類

(1) ファイアウォールなどセキュリティソフトの開発・設定・保守者
(2) ＰＫＩ(Public Key Infrastructure) などのセキュリティシステムの設計・構築を行うシステムエンジニア、システムインテグレータ
(3) 脆弱性診断技術者
(4) 不正侵入検知システムなどの運用者
(5) セキュリティポリシーの作成などを支援するコンサルタント
(6) セキュリティ監査人
(7) セキュリティ教育を実施する人など

JNSAのスキルマップでのスキルレベルのチェックの必要性

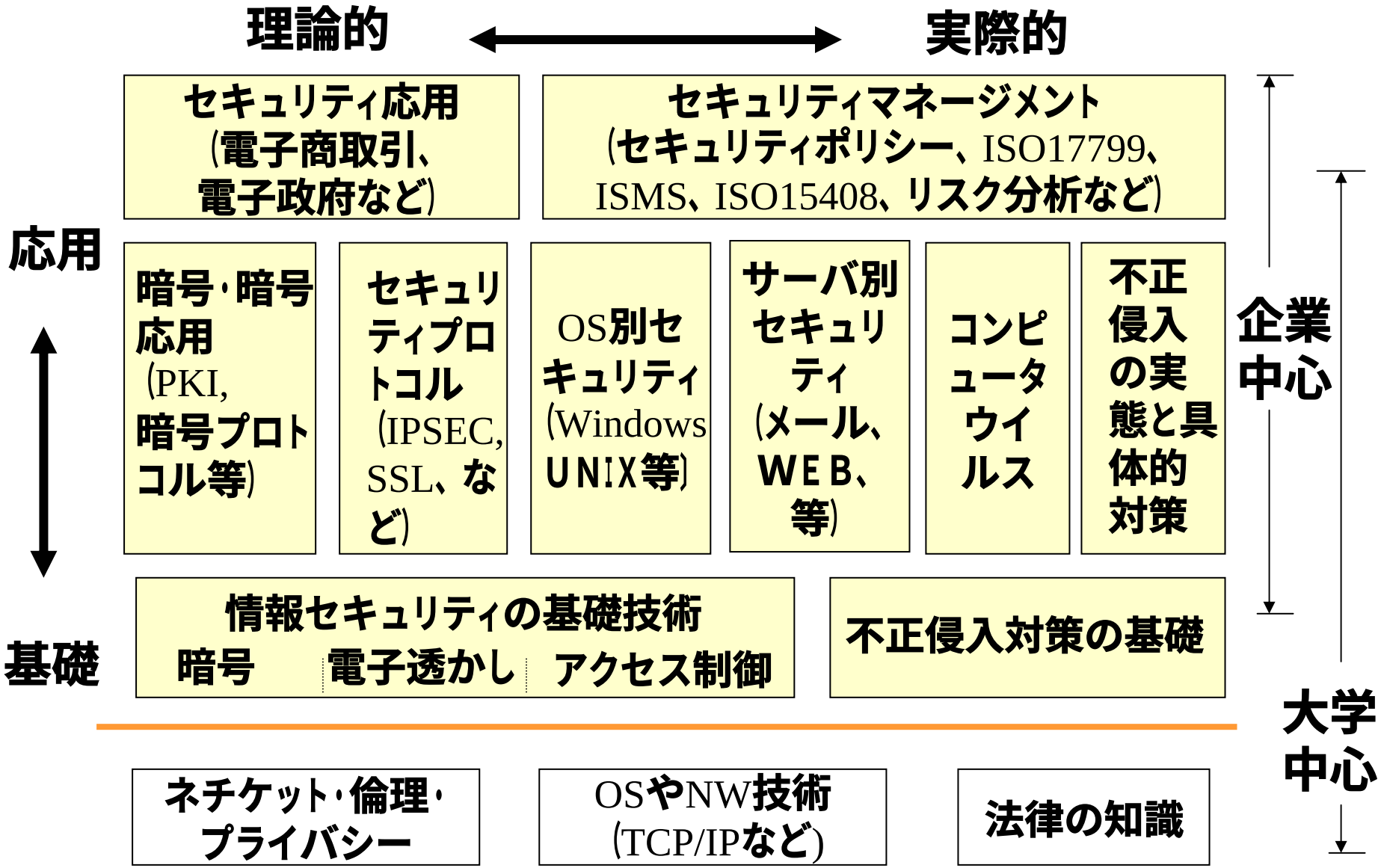


図2　セキュリティ教育の分野

専門企業などにおけるセキュリティ教育

１．米国

（1）RSA**社や**CSI、SANS**などの民間組織で充実した教育を実施。**

（2）米国のセキュリティ専門家認定試験には、ＧＩＡＣ(Global Information Assurance Certification)、CISSP（Certificated Information Systems Security Professional）**試験や、**Security+**試験などがある。**

２．日本

（1）充実しつつあるがまだ玉石混交。

（2）日本における、セキュリティ技術者資格には日本情報処理開発協会が主催する情報セキュリティアドミニストレータ試験の合格者に与えられる資格中心。２００３年よりSEA/J**認定資格立ち上げ。**

海外の大学におけるセキュリティ教育

1．米国

（1） http://avirubin.com/courses.html**に大学におけるセキュリティ教育コースを一覧**

（2）パデゥ大学の修士コースにセキュリティ専攻(学科レベル)

（3）ＣＭＵの修士コースにセキュリティ専攻(学部レベル)2003**年発表**

2．韓国

セキュリティ教育に対して対策が進んでおり学部や大学院に「セキュリティ学科」が誕生し、毎年1000人規模の卒業生を送り出す予定

3．欧州

（1）ＩＣＳＳ（Information and Communication Systems Security）**というEUプロジェクト**

（2）エーゲ大学(ギリシャ）などで上記に基づき大学院で教育を実施

表2　ICSSのセキュリティ教育の項目

Principles of Security and Dependability
Introduction to Cryptography
Information Systems Security
Computer and Communications Security
Formal Software Development
Legal Aspects of Secure Computing
General Systems Theory
Social & Ethical Issues of Secure Computing
Strategic Aspects of I&CT
Network Security
Advanced Cryptography
Technical Realisation of Crypto-algorithms
Security-oriented Project Management
Database Systems Security
Standardisation, Certification & Evaluation
Advanced Network Security

日本の大学におけるセキュリティ教育

(1) 日本の大学におけるセキュリティ教育に関しては、全体の状況を示すサイトがなく全体像がつかみにくい。

(2) 部分的には次のような先進的動きもあるが全体に遅れ気味
　(a) 文科省科学技術振興調整費により、2002年から大阪大学、早稲田大学、2003年より中央大学や工学院大学セキュリティ教育を実施
　(b) 2004年4月より情報セキュリティ大学院大学が横浜に開校することになった。1学年の人数は49人で、情報セキュリティエンジニアや情報セキュリティマネージャ育成を目的としている。

セキュリティ教育に関する活動と考察

(1) 東京電機大学におけるセキュリティ教育
(2) 経済産業省における情報セキュリティ教育
研究会座長

東京電機大学における セキュリティ関連教育

1．「情報倫理」工学部1－4年生　2001年より約200名/年

被害者にも加害者にも犯罪者にもならないための方法

教科書：佐々木「インターネットセキュリティ入門」岩波新書、1999年

2．「コンピューティング基盤とセキュリティ」工学部情報メディア学科4年生　2005年より

セキュリティへの脅威とセキュリティ対策技術の概論

教科書：佐々木他「インターネットセキュリティ　基礎と対策技術」オーム社、1997年

3．「ネットワークセキュリティ特論」工学系大学院生

2001年より約90名/年

暗号と電子透かしを中心にしたセキュリティ技術の特論

教科書：佐々木他「インターネット時代の情報セキュリティ　暗号と電子透かし」共立出版、2000年

大学院でのセキュリティ教育の私の考え方

(1) 大学における教育の内容を決定するにあたっては,
　(a) 直接的に役に立つ事と共に、
　(b) 大学でなければできない基礎からの積み重ねを必要とする物に重点をおく事が必要である。
(2) 役に立つと言う意味においては、
　(a) ウイルス対策
　(b) 不正侵入の実態と対策
　(c) セキュリティプロトコル
　(d) セキュリティマネージメント
(3) 基礎からの積み重ねを必要とすると言う意味においては、
　(a) セキュリティ技術の基礎 (暗号技術、電子透かし技術など)
　(b) 暗号応用技術 (電子署名・暗号プロトコルなど)
(4) 役に立つためには実習が不可欠
(5) 教育の範囲が広く一人の教員では非常に困難ー＞SEA/J
(6) 大学院生と社会人が一緒に学ぶことによりシナージ効果が期待できる。ー＞社会人の受講許可

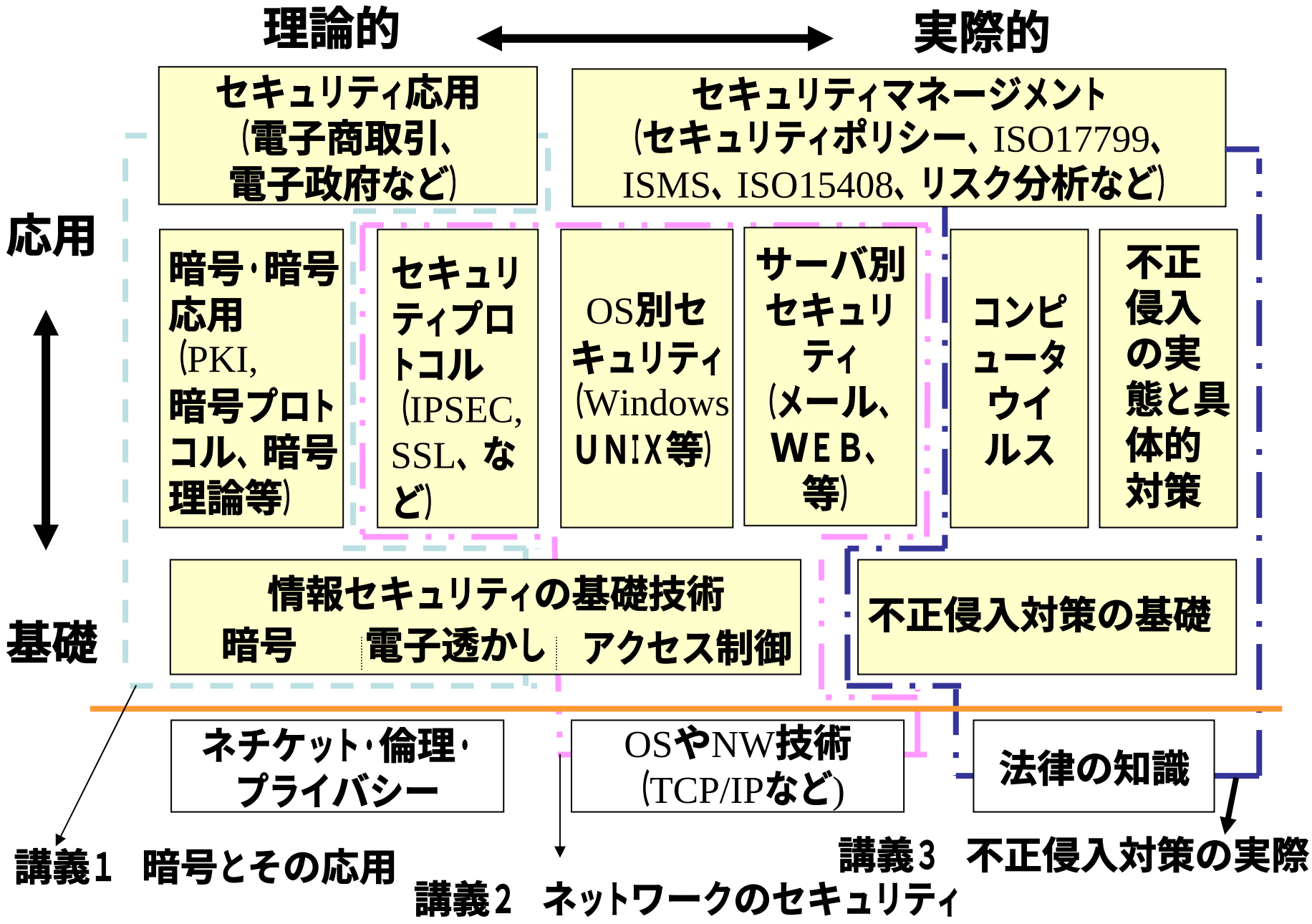


図　電機大大学院における今後の講義案

講義１（暗号とその応用）全体計画（前半）

第1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、セキュリティへ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2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3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。

４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5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6回　公開鍵暗号２：公開鍵暗号として、エルガマル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。

講義１（暗号とその応用）全体計画（後半）

第7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8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9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10回　暗号プロトコル：暗号をベースにした秘密分散法や、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11回　不正コピーの防止技術：技術の概要、電子透かしなど
第12回　全体のまとめ：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。

講義2（ネットワークのセキュリティ）全体計画

対象：学外の技術者，大学院生
講義形態：通常の講義形態＋実習
講師：学外講師中心（SEA/J）

第１回　イントロダクション
第２回　ネットワークセキュリティ技術の概要
第３回　不正侵入の現状と対策の基礎
第４回　ウイルス対策
第５回　**メール･WEBセキュリティ**
第６回　**クライアントOSセキュリティ対策**
第７回　セキュリティプロトコル（SSL,IPSEC)
第８回　不正侵入と対策技術
第９回　アクセス制御
第１０回　ネットワークセキュリティトータル設計
第１１回　セキュリティマネージメント
第１２回　全体まとめ

講義３（不正侵入対策の実際）全体計画

対象：学外の技術者，管理者，大学院生
講義形態：通常の講義形態＋実習
講師：学外講師中心（SEA/J）

第１回　イントロダクション
第２回　セキュリティマネージメント
第３回　ウイルス対策
第４回　Windowsセキュリティ
第５回　UNIXセキュリティ
第６回　セキュリティプロトコル
第７回　ソフトウエア開発とセキュリティ
第８回　不正侵入と対策技術１（IDSの構築、検出実習）
第９回　不正侵入と対策技術２（アクセス制御、NAT、FW等)
第１０回　ケーススタディ
第１１回　情報セキュリティと法律
第１２回　全体のまとめ

大学院講義の対象と方法

	対象		講義法			講師	
	大学院生	社会人	通常	実習	E	大学	企業
講義1 (暗号とその応用)	約50人	15人	◎	○	○	佐々木 ◎	○
講義2 (ネットワークのセキュリティ)	15人	15人	○	◎	○	◎	◎
講義3 (不正侵入対策の実際)	15人	15人	○	◎	○	SEA／J ○	◎

講義2と3についてはＳＥＡ／Ｊに講師の派遣依頼

E:E-ラーニング　　通常：通常の講義

経済産業省情報セキュリティ教育研究会

1．目的：組織の情報セキュリティを維持・向上させる責任と権限を実質的に負うべき実施責任者、すなわち「企業等における情報システム関連部署の長」、「大学等におけるメディアセンター長」、「ISMS でいうところの情報セキュリティ委員会の委員長や、CISO等を補佐する立場にある者」等を育成するための情報セキュリティ教育のあるべき姿を検討する。

2．期間：2003年度4回の会合とWG活動

3．研究会メンバー：学識経験者など15名（座長：佐々木）

4．主要な実施事項：
（1）カリキュラム案作成
（2）ケース別教育コース案提案
（3）セキュリティ教育に関する提言

個人としての提言

(1) 組織の責任者 (経営層) への注意喚起 (民中心)

すべての組織の責任者は、情報セキュリティ教育の重要性を再認識し、自ら主体的に情報セキュリティ実現のための行動を起こすこと。

(2) 情報セキュリティ教育の推進主体の設立 (官・民)

情報セキュリティ関連技術等の進歩に合わせて、常に最適な教育のあり方を検討・整備するために必要な体制を整備すること。

また、ユーザ企業が自ら積極的に教育を推進するために、そうした主体的な行動を支援する枠組みを整備すること。

(3) 情報セキュリティに関連するスキル維持のあり方の検討 (官中心)

情報セキュリティに関連する各種の試験体系を見直し、必要に応じて情報処理技術者試験制度における試験の新設や改訂、また民間資格試験制度の活用等の方策を検討すること。

セキュリティ教育とJNSA

1．スキルマップWG
2．ITSS実証実験評価WG

スキルマップWGの活動

リーダー佐久間　敦氏（富士総研）

- 情報セキュリティ人材の育成に向けて「情報セキュリティのためのスキルマップ」を作成
- スキルマップをベースに、情報セキュリティ人材の育成や評価の方法について検討
- 情報処理推進機構（IPA）の支援を得て，以下の調査研究事業を実施
  - 「情報セキュリティプロフェッショナル育成に関する調査研究」（H14年度）
  - 「情報セキュリティスキルマップ構築の調査研究」（H15年度）

「スキルマップ」について

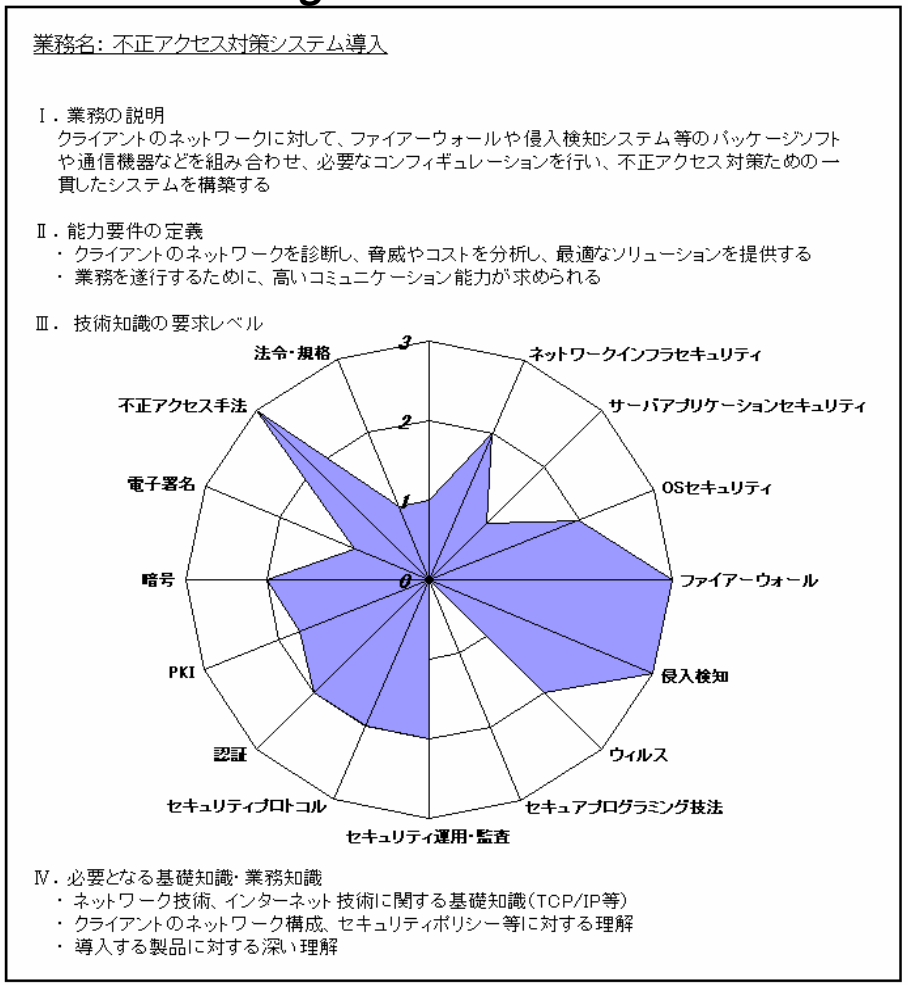
- 情報セキュリティの技術知識を16の大分類に整理
- 技術知識の習得の度合い（レベル）を定量的に表現する「評価のものさし」を目指す

1. 情報セキュリティマネジメント		7. ウイルス
2. ネットワークインフラセキュリティ		8. セキュアプログラミング技法
3. アプリケーションセキュリティ	Web	9. セキュリティ運用
	電子メール	10. セキュリティプロトコル
	DNS	11. 認証
4. OSセキュリティ	Unix	12. PKI
	Windows	13. 暗号
	Trusted OS	14. 電子署名
5. ファイアウォール		15. 不正アクセス手法
6. 侵入検知システム		16. 法令・規格

スキルマップの展開

- スキルモデル
  - 個別の業務やタスクにおいて求められるスキルとレベルを整理
  - 人材育成や採用、能力評価、調達など、幅広い用途に活用
- スキルレベルチェックリスト
  - 自己評価を行うための問題と解答のリスト
  - スキルマップの16大分類ごとに各10問（合計160問）のサンプル問題を作成

Fig. スキルモデル



ITSS実証実験評価WGの活動

リーダー：松田　剛氏/ヒューコム

1．WGの活動目的

ITSS実証実験の教育効果の測定評価を目的としていて、その成果を今後の セキュリティ技術者の評価基準策定にも利用できることを目指す。

2．WGの年間活動予定

2003年9月から12月まで、ITSS実証実験に併せて、教育評価方法を 検討する。

セキュリティ教育参考文献

1) 佐々木良一「情報セキュリティ教育を俯瞰する」Cyber Security Management誌、Vol3,No.30 (2002年4月号)

2) 佐々木良一、杉立淳 「情報セキュリティ教育の現状と今後」電子情報通信学会 技術と社会・倫理研究会、2003年2月

3) 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，pp30-40，No.15, 2003

4) 米国のセキュリティ教育コース http://avirubin.com/courses.html

5) 西山裕行「ネットワークを介したセキュリティ遠隔システムの開発と実践」情報処理学会2001年度秋期全国大会

6) SANS関連：http://www.sans.org/index.php

7) 土居範久監修、佐々木良一代表編者「情報セキュリティ事典」、共立出版、2003年 (http://www.kyoritsu-pub.co.jp/kinkan/shosai/kin12070-1.html)