情報セキュリティ人材育成について

2005年3月17日

次世代IPインフラ研究会

セキュリティワーキンググループ

情報セキュリティ大学院大学　兼　中央大学 研究開発機構
内田　勝也（uchidak@gol.com）

情報セキュリティ人材育成について

はじめに・・・

- 1998年6月 NETSEC'98 (CSI 主催) キーノートスピーチ
  Purdue大学のEugene Spaffordは、「いわゆるハッカーを雇う必要はない。我々の大学の学生は、ハッカーに対して優とも劣らない」
- 2000年10月：米国SANS. ORG主催「Firewall講座」(5日間) に参加。 講師のレベルの高さ、受講者数 (約500名：全体では2000名程度？) に愕然
- 2001年4月：共立出版より、「情報セキュリティ事典」刊行の話があり、編集委員の一人として参加、企業の技術者・管理者教育を2001年末に執筆 (刊行は2003年7月)
- 2002年6月：日本セキュリティマネジメント学会 全国大会にて、「技術者・管理者向け情報セキュリティ教育試案」を発表した。
- ハッカーを雇うべきとの考えがマスコミ等の報道では多いが、ハッカーをコンサルタントとして雇用するかとの回答では、米国15%、日本1%となっている。(米国：CSI/FBI、日本：小職の調査)

Eugene Spafford：
「UNIX & インターネットセキュリティ」の著者の一人。1988年の「インターネットワーム」事件の対応を行った一人
(ACMの特集「The Worm Story」で "Crisis and Aftermath"を執筆)

CSI
COMPUTER SECURITY INSTITUTE

NETSEC'98： (http://www.gocsi.com/)
米国コンピュータセキュリティ団体CSI (Computer Security Institute) 主催の国際会議・展示会の1つ (毎年6月開催で、今年は15回目) で、11月開催のAnnual Conf. & Exhibitionは今年 (2005年) で32回目 (第1回は1974年) になる。

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

情報セキュリティ 人材育成の必要性

- e-Japan計画を始め、安全で信頼できる電子社会の推進にセキュリティ技術者・管理者の育成は喫緊の課題。
- 国内の大学・大学院の育成体制は十分でなく、既存の民間企業主催の教育は断片的なものが多い。
- 情報セキュリティ分野も「Dog year」で進展しており、常に知識・技術の更新が必要。
- 情報セキュリティは総合科学であり、
  - 技術
  - 管理・運用
  - 法制度

  を含め、総合的な指導を理論・実践の両面から情報セキュリティ要員の育成を図ることが重要。
- 国内では、一部の大学での取り組みが始まっているが、要員育成従事者の不足は深刻。
  1. 大阪大学「セキュア・ネットワーク構築のための人材育成」
  2. 早稲田大学「セキュリティ技術者養成センター」
  3. 中央大学 21世紀COE「電子社会の信頼性向上と情報セキュリティ」
  4. 中央大学「情報セキュリティ・情報保証 人材育成拠点」
  5. 工学院大学「セキュアシステム設計技術者の育成」
  6. 情報セキュリティ大学院大学 修士課程（2004年4月開校）
  7. カーネギーメロン大学 情報大学院（2005年9月開校）

  （注）①②④⑤は、文部科学省科学技術振興調整費によるもの

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

情報セキュリティ 人材育成の必要性

- 国内の資格試験の特徴
  - 国内固有のものは取得すれば、有資格者となり剥奪はない ⇒ 30年前のものでも有効！
  - 海外の資格の多くは、有期で一定の継続教育を受けると更新可能なものと有期で更新なしのものがある
- 資格試験
  - 情報処理技術者試験 更新なし
    - 情報セキュリティアドミニストレータ試験
    - システム監査技術者
  - NISM (Network Information Security Manager、ネットワーク情報セキュリティマネージャ) 2年更新
  - SEA/J (Security Education Alliance/Japan) 更新なし
    - 基礎コース
    - 応用コース (テクニカル／マネジメントの2種類)
  - CISSP (Certified Information Systems Security Professional) 3年更新
  - CISM (Certified Information Security Manager 公認情報セキュリティマネージャー ISACA主催) 3年更新
  - GIAC (Global Information Assurance Certification SANS主催) 2年～4年更新
    - Security Essentials Certification (GSEC)
    - Certified Intrusion Analyst (GCIA)
    - Certified Windows Security Administrator (GCWN)
    - Systems and Network Auditor(GSNA)
    - Information Security Fundamentals (GISF)
    - Certified ISO-17799 Specialist (G7799)
    - Certified Security Consultant (GCSC)
    - .Net (GNET)
    - Information Security Officer (GISO)
    - Certified Firewall Analyst (GCFW)
    - Certified Incident Handler (GCIH)
    - Certified UNIX Security Administrator (GCUX)
    - Certified Forensics Analyst (GCFA)
    - Security Audit Essentials (GSAE)
    - Security Leadership Certification (GSLC)
    - Secure Internet Presence (GSIP)
    - Operations Essentials Certification (GOEC)

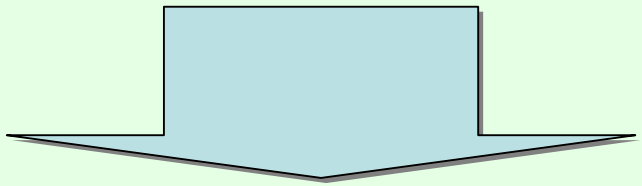
Katsuya Uchida uchidak@gol.com

情報セキュリティ 人材育成について

情報セキュリティ 人材育成の必要性

- 資格試験
  - シマンテック認定技術者資格　2年更新
    - テクノロジーアークテクト
    - セキュリティエンジニア
    - セキュリティプラクティショナー

    } シマンテック ソリューション試験 ＋ ベンダーニュートラル資格
  - Security+（主催 CompTIA）　更新なし



- 有期のものは以下の特徴があると思われる。
  - 更新を行う組織を持っている
  - 新たな技術への対応ができている
  - 教育体制が確立されている
  - 財政的に安定しているためと思われる

変化の激しい情報セキュリティ分野では
有期にすべきではないだろうか？

Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

米国の情報セキュリティ 人材育成

- 米国では、ＮＳＡ が運営しているＮＩＥＴＰ (National Information Assurance Education and Training Program) と呼ばれる教育･訓練プログラムがあり、広範なサービスを提供
- NIETPプログラムに、CAEIAE (The National Centers of Academic Excellence in Information Assurance Education)と呼ばれる情報セキュリティの21世紀ＣＯＥ版がある
- 制度は、PDD63 (大統領指令６３) の報告を受けて始められた
  ＰＤＤ６３： 1998年5月にクリントン大統領が発令。NIPC、ISAC等が創設された。
- ４年生の大学生と大学院生が応募できるようになっており、CAEIAEコースに参加している学生は、奨学金制度の申込み権利があり、国防総省情報保証奨学金プログラムやSFS (Federal Cyber Service Scholarship for Service Program) プログラムへの権利を与えられる
- SFSでは、奨学金を最大２年間、必要な全ての経費、書籍、授業料、部屋代など、に当てることができる。更に、給付金として、学生は年間最大8,000ドル、大学院生は年間最大12,000ドルが与えられる
- 奨学金を受け取った学生は、奨学金受給期間か１年のいづれか長い期間、連邦機関 (Federal agency) に勤務しなければならない

大学･大学院に対して補助金をだすのではなく、**基準を満たした大学･大学院に入学する学生･大学院生に対して援助**する仕組みになっており、また、卒業後は一定期間、政府系機関に勤務することを義務づけている

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

シンガポールの情報セキュリティ人材育成

- CITREP（Critical Infocomm Technology Resource Programme）プログラムと呼ばれており、情報通信開発庁（IDA: Infocomm Development Authority）が対応
- 情報通信業界やユーザ企業が必要とする情報システム（含 情報セキュリティ）教育訓練に対してインセンティブを与えるもの
- 教育訓練だけでなく、資格試験も含めて対象になる
- 教育訓練に対しては最大70%（S$3，500：約23万円）まで補助
- 資格試験に対しては最大70%（S$1，000：約6．5万円）まで補助
- 資格試験例（情報セキュリティ関係のみ　一部分）

CISSP CBK Review Seminar
Check Point Certified Security Administrator & Certified Nokia Security Administrator - ECS (VPN-04)
Computer Hacking Forensic Investigator
CSPFA CISCO Secure PIX Firewall Advanced
Developing Secure Internet Applications
eXtreme Hacking
Linux Network Administration and Security
Securing Cisco IOS Networks

Security Certified Network Professional (SCNP)
Security Technology and Management Course (eSTEEM)
Sun Certified Security Systems Administrator - IM
Sun Certified Security Administrator for the Solaris Operating Environment - ECS (SC-300)
Sun Network Intrusion & Detection - ECS (SC-345)
Ultimate Hacking
Web Application Security Training

http://www.ida.gov.sg//idaweb/training/infopage.jsp?infopagecategory=factsheet:training&versionid=6&infopageid=119

Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

米国の情報システム人材育成数

- 米国商務省発表資料（１９９９年）

単位：千人

	１９９６年	２００６年			
		1996 BaseYear Employment	Net Replacements	New Jobs	Total
Computer Scientists	212	193	19	249	461
Computer Engineers	216	201	15	235	451
Systems Analysts	506	471	34	520	1,025
Computer Programmers	568	391	177	129	697
Total	**1,502**	**1,063**	**245**	**1,378**	2,634

１９９６年から２００６年までの１０年間で、１５０万人が２６０万人に増加すると想定している。
このため、毎年１３７，８００人の増加が必要となる。
情報セキュリティ技術者は、Scientistsに分類されている。もしScientistsの５％程度が情報セキュリティ技術者だと考えると、ハイレベルな情報セキュリティ技術者は、年1,２４５人の要員育成が必要。

http://www.technology.gov/Reports/TechPolicy/digital.pdf

- 日経IPプロフェショナル（２００４年６月調査）
  - ２万人超のITエンジニアの４６％が、「人の助けを借りながら業務を遂行できる」エントリーレベル（ITエンジニアではない！ 素人がIT業務らしきことを行っているだけ？）
- シンガポール開催のセキュリティ会議（２００４年１０月 CSI-Asia）
  - ４００～５００名が有料会議（ＵＳ＄６００ドル）に参加。大分部はシンガポールから
- 大学院
  - カーネギーメロン大学 日本校 初年度：２０名定員　２～４年度：５０名　５年度以降：１００名
  - 情報セキュリティ大学院大学：　４９名
  - その他

Katsuya Uchida　uchidak@gol.com

人材育成への対応

米国ＮＳＡやシンガポールＩＤＡ等の対応を考えると

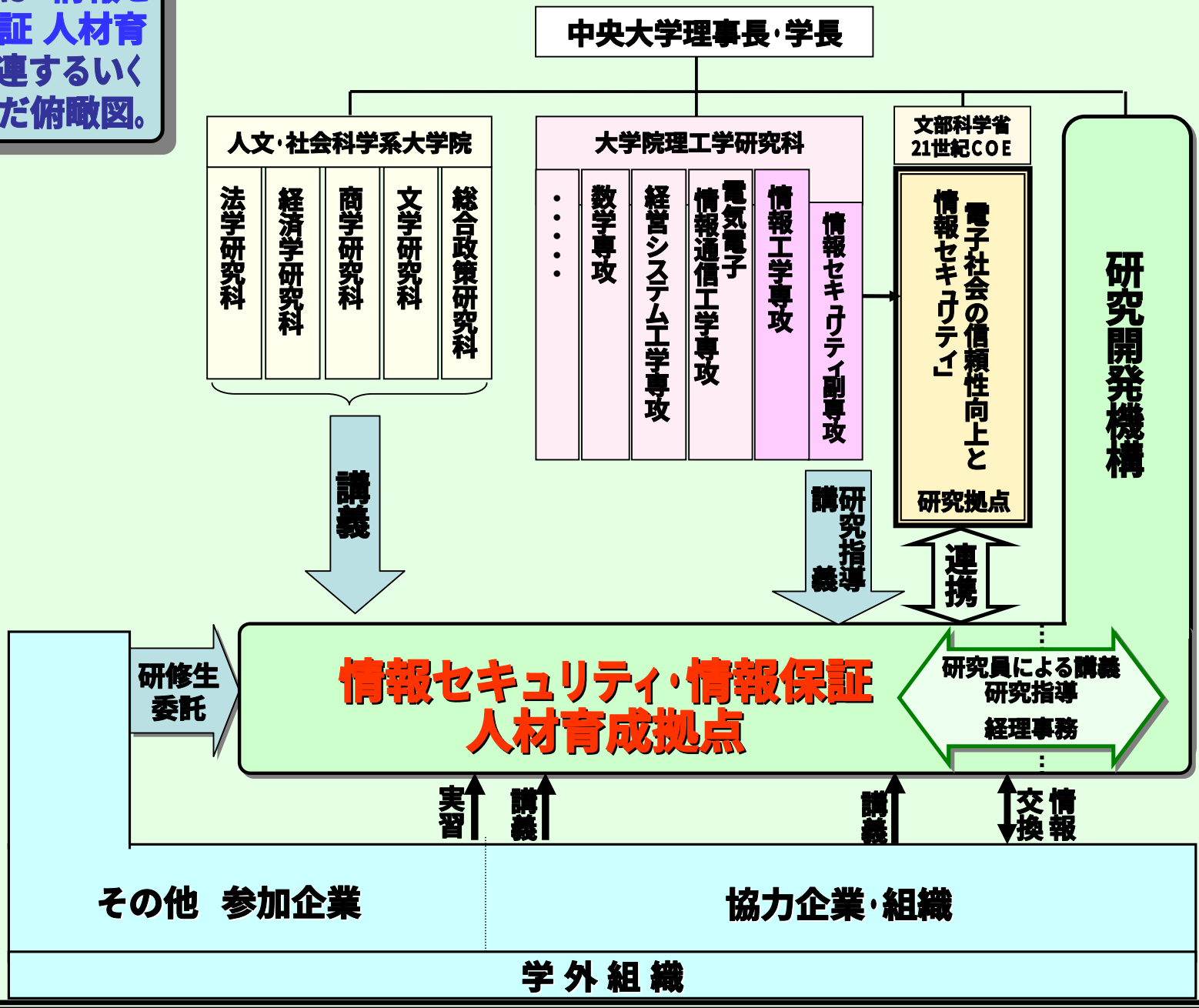
- 人材育成への支援は、個人、法人？
  - 基本としては個人を考えるべきではないか
  - 国内の環境や情報セキュリティの特性を考えると、中小企業等への支援は必要であろう
  - 大都市圏から遠い地域の企業への対応も必要であろう
- 教育研修参加や資格取得への対応
  - 有期資格を対象とする（？）
  - 専修学校、専門大学院、大学、大学院は？　・・・ 米国ＮＳＡ方式で対応する？
  - 研修コース、資格については、第三者機関（？）にて審査が必要であろう。
  - 政府は、審査結果の認定と費用に対する助成を行う？

Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

参考：中央大学情報セキュリティ俯瞰図

現在、中央大学では「情報セキュリティ・情報保証 人材育成」だけでなく、関連するいくつかのものを含んだ俯瞰図。



Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

参考：中央大学 情報セキュリティ副専攻

中央大学における副専攻制度

- 大学院教育の目的が、従来の研究者養成から実務家の養成に移ってきた。
- 新しい学問の成果の吸収、分野横断的な教育、理学と工学の融合など、これまでになかったカリキュラムを提供する。
- 副専攻として、「情報セキュリティ」、「防災・危機管理工学」、「環境理工学」、「データ科学」、「ナノテクノロジー」の５副専攻を設けた。
- 副専攻は、博士課程前期程度、同後期課程に設置し、十分な教育・研究上の指導体制を整備。
- 副専攻を履修することで、専攻分野の学問に加え、異なる分野の知識や見識を身に付けることが可能になった。

情報セキュリティ副専攻制度

- 学際的カリキュラムを編成した。
- 大学の諸学科の卒業生、産業界や自治体等政府系機関の情報システム管理者・技術者など広い層を対象とした電子ビジネスや電子政府・自治体あるいは電子医療等の分野における人材の育成を図ることを狙いとした。
- 修了要件は、特別演習Ⅰ・Ⅱ（4単位＋リサーチペーパー）及び必修科目（１０単位）を取得。

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

参考：中央大学 情報セキュリティ副専攻

カリキュラム

科　目	単位数	開講	内　　容	必修選択
電子社会と情報セキュリティ	2	半	電子社会の定義、理念等について考察した後、我が国及び先進各国の現状と動向について説明する。	必
暗号と電子認証	2	半	暗号の役割は秘匿と認証にあり、暗号方式として2つの方式、即ち、共通鍵暗号方式と公開鍵暗号方式があるが、これらについて技術面からの解説を行う。 電子行政や電子ビジネス、あるいは電子医療などあらゆる電子社会システムの基盤が、人、文書、モノ、金等に関するあらゆる情報の真正性を保証することににについて説明を行う。 真偽の峻別という認証機能が主として公開鍵暗号によるデジタル署名によって行われることを説明し、具体的な暗号の利用例として電子投票方式について解説する。	必
ネットワークセキュリティ	2	半	セキュリティ要素、情報倫理、アクセス制御、有害プログラム、ファイアウォール、VPN (Virtual Private Network) 侵入検知システム、セキュリティポリシー、リスク分析、Windowsセキュリティ、UNIXセキュリティ、ISO15408やISMSなどのセキュリティ評価･認証基準、セキュリティ監査、暗号、法制度の概要などについて解説を行う。	必
システム監査Ⅰ	2	半	セキュリティ監査の歴史について述べ、情報システムの監査を中心に、信頼性監査、安全性監査、効率性監査、監査証拠と監査証跡、システム監査技術、システム監査の主体、監査対象、独立性等について説明	必
システム監査Ⅱ	2	半		選
情報セキュリティ法制Ⅰ	2	半	サイバー犯罪の現状について概説する。個人情報保護に関する法律案や電子署名及び認証業務に関する法律、商業登記法 (改正) 、不正アクセス禁止法、著作権法 (1999年改正) 等の法整備の現状と動向について解説を行う。	必
情報セキュリティ法制Ⅱ	2	半		選
情報セキュリティ特別演習	2	半	リサーチペーパー作成	必
	2	半		必

Katsuya Uchida　uchidak@gol.com

参考：中央大学 21世紀COE

21世紀COEとは？

- 21世紀COEプログラムとは、第三者評価に基づく競争原理により、世界的な研究教育拠点の形成を重点的に支援し、国際競争力のある世界最高水準の大学づくりを推進するためのプログラム。
  http://www.mext.go.jp/a_menu/koutou/coe/index.htm
- 2002年度に中央大学 辻井重男教授を拠点リーダーとする「電子社会の信頼性向上と情報セキュリティ」が情報セキュリティに分野で採択された。
- 故意(悪意)のみならず、災害、故障、過失も可能な限り考慮して電子社会の信頼性と情報セキュリティを向上させるための技術的対策を中心とした総合的研究を推進している。
- 研究対象については、大きく分類すると、
  - 総論(電子社会における安全学の構築)
  - 電子社会システム層
  - 高信頼ネットワーク・システム層
  - 要素技術層

  人文社会科学的視点、技術と理論からの視点など、広範囲から問題を捉えることを目的としている。
- 第Ⅰ層(要素技術層)では、代数曲線を利用する公開鍵暗号の研究、個人識別技術、量子暗号など電子社会を構築するための要素技術を研究する。
- 第Ⅱ層(高信頼ネットワーク・システム層)は、要素技術と電子社会を有機的に結びつけるために必要なネットワーク構築技術、PKI (公開鍵基盤)関連技術、更に管理・運用に関する研究も行う。
- 第Ⅲ層(電子社会システム層)では、行政・ビジネスの電子化などを視野に入れた応用研究を中心に行う。また、研究の後半(2005年度頃)からは、図：中央大学21世紀COEプログラム「電子社会の信頼性向上と情報セキュリティ」研究対象学術・文化・産業ネットワーク多摩や中央コリドー高速通信実験協議会のネットワークを活用したアンケートシステムの技術的・社会的実験も予定している。
- COEのウェブページ：　http://www.21coe.chuo-u.ac.jp/

Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

参考：中央大学 21世紀COE

人文・社会科学的視点からの助言・評価

法学
経済学
商学

総論（電子社会における安全学の構築）

第III層

電子社会システム

電子行政　　：　電子投票・アンケートシステム
電子ビジネス：　電子マネー、電子証券システム
　　金融情報システム
　　地理情報ネットワークシステム
電子データの信頼性向上

第II層

高信頼ネットワーク・システム

高機能・高信頼ネットワーク構成
電子認証・公証システム、ネットワークセキュリティ
セキュリティポリシー・運用管理

政策
経営
情報社会論
情報倫理

代数幾何
整数論
統計学
アルゴリズム
計算量理論
計算幾何
数値計算

第II層

要素技術

代数曲線を利用する公開鍵暗号（楕円・超楕円暗号）
公開鍵暗号の安全性証明　共通鍵暗号の強度評価
統計的手法による乱数検定　DNA情報による個人識別マルチパーティプロトコル　量子暗号
電磁波漏洩とその可視化

画像処理
可視化技術
知識処理
データベース
システム監査

情報セキュリティを支える理論と技術

Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

参考：中央大学 21世紀COE

「COEプログラム」での教育拠点

- 社会人博士後期課程学生（企業等に在籍のまま入学）の積極的受け入れによる、産業界との交流。
- COE を中核とし理工学研究科及び研究開発機構との共同あるいは一体的研究を通じての人材育成。
- 理工学研究科における情報セキュリティ副専攻(博士前期・後期課程)の設置による人材育成。
- 全学的組織として設置を目指している独立研究科「電子社会システム研究科」において、情報セキュリティコースを設けて広い視野からの情報セキュリティ分野の人材育成。
- 工学と数学、工学と人文・社会科学との学際的研究を通じて深い専門性と広い視野を持つ人材の育成。
- 「本COEプログラム」では、２００２年度からCOE研究員、ポスドク、リサーチアシスタント(博士後期課程学生)の採用を行い、２００３年度は、研究員4名、ポスドク2名、更にリサーチアシスタントを10名程度採用する予定になっている。また、社会人博士後期課程学生数名を受け入れ、人材育成を目指す。

「COEプログラム」での研究活動

- 世界的な研究教育拠点の形成を目指し、国内外の研究者の交流を目的とした研究会やシンポジウムの開催。
  開催案内、講演資料は下記ＵＲＬ。

  http://www.21coe.chuo-u.ac.jp/security/index.html

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

参考：パーデュー大学 修士コース

- ８０年代後半から始まっており、この分野では最も歴史が長く、内容も充実している。
- コンピューターサイエンス (CS) 専攻の一つとして行われている。
- ３単位の講座を①１０講座を履修するか、②8講座と論文を履修する。
- 以下の三つの必須コースを履修しなければならない。
  - アルゴリズム (Algorithms)
  - システムⅠ (コンパイラーとプログラム言語)
  - システムⅡ (ネットワークとオペレーティングシステム)
- 表1に示されたコースの講座番号から、４講座を選択する
- 論文を選択しない場合には、表2に示す500番台、600番台の講座から更に3講座を、論文を選択した場合には、１講座を選択する

分　野	コース	
Algorithms	CS580	
Systems I (Compilers and Programming Languages)	CS502、565	
Systems II (Networks and Operating Systems)	CS503、536	636、638
Artificial Intelligence	CS572	
Complexity	CS584	
Databases	CS541、542	641
Geometric Modeling, Visualization, and Graphics	CS530、531、535、586	
Numerical Computing	CS514、515、520	614、615
Parallel and Distributed Computing	CS525	603
Security	CS526、555	626、655
Simulation and Modeling	CS543、544	
Software Engineering	CS510	

表1　パーデュー大学 修士コース

Purdue大学　　http://www.purdue.edu/

Katsuya Uchida　uchidak@gol.com

情報セキュリティ人材育成について

参考：パーデュー大学 修士コース

CS526 : Information Security

• Introduction: Role of security, Types of security, Definitions.	◆ 入門：セキュリティの役割、セキュリティの種類、定義
• Classification Schemes, Access Control	◆ 情報資産分類、アクセス制御
• Formalisms: Information flow, Protection Models	◆ 形式論：情報フロー、保護モデル
• Policy: Risk Analysis, Policy Formation, Role of audit and control	◆ ポリシー：リスク分析、ポリシー構成、監査及び管理の役割
• Formal policy models.	◆ 正規のポリシーモデル
• Cryptography: Cipher methods, Key management, digital signatures	◆ 暗号：暗号化方法、鍵管理、電子署名
• Authentication and Identity	◆ 認証と識別
• System Design principles. TCB and security kernel construction, Verification, Certification issues	◆ システム設計原則、ＴＣＢとセキュリティカーネル構築、検証、認証
Midterm Exam	
• System Verification	◆ システムの検証
• Network Security. Distributed cooperation and commit, Distributed authentication issues. Routing, flooding, spamming. Firewalls	◆ ネットワークセキュリティ、分散型協調とコミット、分散認証、ルーティング、フラッディング、スパム、ファイアウォール
• Audit Mechanisms	◆ 監査
• Malicious Code: Viruses, Worms, etc.	◆ 有害プログラム：ウイルス、ワーム等
• Intrusion Detection and Response	◆ 侵入検知と対応
• Vulnerability Analysis	◆ 脆弱性分析
• Physical threats, operational security, Legal and Societal Issues	◆ 物理的脅威、オペレーションセキュリティ、法的･社会的課題
Final Exam	

Katsuya Uchida uchidak@gol.com

参考：パーデュー大学 修士コース

パーデュー大学の修士コース

- 情報セキュリティを専攻するのであれば、表2に示した「情報セキュリティ（Information Security）」、「暗号学（Cryptography）」、「情報保証特論（Advanced Information Assurance）」、「応用暗号学（Advanced Cryptology）」等の講座を選択する。
- 更に表2には、「CS590D 分散システムにおけるセキュリティ概要（Security Aspects in Distributed Systems）」、「CS590E 情報セキュリティの最新の話題（Topical Lectures in InformationSecurity）」、「CS590U アクセス制御：理論と実際（Access Control：Theoryand Practice）」等の講座が用意されている。
- 情報セキュリティを専攻する場合、単に**情報セキュリティ関係だけでなく、OSやコンパイラー等の履修を求めている**のも米国の情報セキュリティ専攻での特徴といえる。

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

参考：カーネギーメロン大学日本校

- CMU情報工学修士ー情報セキュリティ(MSITーIS)
- 2005年9月開校予定
- Carnegie Mellon CyLab、Heinz III Schoolの公共政策･管理、Information Networking Instituteが兵庫県と共同で開校するもの。
- MSITーISのカリキュラムは、情報セキュリティの分野で指導者や管理者 (CSO : Chief Security Officer) に必要なセキュリティ技術や分析手法とともに、企業経営･方針に関する包括的な教育を実施し、専門能力と実践的な経営能力を兼ね備えた人材の育成を目指します。
  また、MSIT-ISの学生はCMUの世界的に名高い教授陣や研究者とプロジェクトを遂行する機会を持つことになります。
- このコースでは、CISO (Chief Information Security Officer) として必要な教育を目指している。
  - 組織が直面する情報セキュリティリスクの評価
  - これらのリスクに関連する技術的及び人間的な問題の理解
  - リスクを防ぎ、システムの脆弱性を和らげ、業務を復旧させるためのツール類や手続きの評価
  - 安全な情報基盤の開発、取得、評価についての管理
  - 複雑なシステム及び組織的な目的のための情報セキュリティポリシー、法的環境、市場開発の評価
  - 情報セキュリティ分野における長期にわたる学習意欲と専門分野の深耕を自分自身に課すことができること

http://web.pref.hyogo.jp/johosec/cmuj/details.htm

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

参考：カーネギーメロン大学日本校

- **学位取得に必要な単位**

必修科目	選択科目	プロジェクト	合計
60単位	60単位	24単位	144単位

- **カリキュラム**

情報工学系と公共政策経営系の2つの教育機関のカリキュラムを融合し、体系化した学際的なカリキュラム。選択科目は、開講までにさらに増加します。なお、提供科目は、今後変更することがある。

必修科目（6科目・60単位）	選択科目（60単位を選択）
（1）通信ネットワーク概論 （2）情報セキュリティ概論 （3）セキュリティアーキテクチュア及び分析 （4）情報セキュリティのリスクマネジメント （5）IT管理者のための統計学 （6）不確定環境状態における意志決定	（1）ネットワークセキュリティ （2）ソフトウェアエンジニアのためのセキュリティ （3）デジタル時代のプライバシー （4）データベースマネジメント （5）通信マネジメント
プロジェクト(派遣企業から提案のあった課題等を共同研究) 24単位 合計 144単位	

※ 上記に加え、日本の社会制度に適応し、実務面に重点を置いた日本校独自科目を開講予定

http://web.pref.hyogo.jp/johosec/cmuj/cmuj_index.htm

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

参考：カーネギーメロン大学（米国）CISO短期コース

- 下記の各コースは3日間の授業になっており、費用は各2,400ドルで、このコースを終了するとCMUの修士コース（MSIT-ISP）の24～48単位の履修とみなす
  - Smart Budgeting, Spending & Metrics
  - Law, Investigation, Ethics & Privacy
  - Strategic Planning & Leadership
  - Organizational Management & Negotiation Strategies
  - Risk Management & Business Continuity Planning
  - Physical Security
  - Information Security
  - Key Technologies & Emerging Trends

Katsuya Uchida uchidak@gol.com

情報セキュリティ人材育成について

参考： 情報セキュリティ大学院大学

カリキュラム

技術・管理運営・法制度・情報倫理を相互に連携、協調させた、横断的で創造的な情報セキュリティ教育を目指している。

	授業科目名	履修区分	単位数	修了に必要な単位数
専門基礎	情報デバイス技術	選択	2	8
	プログラミング	選択	2	
	インターネットテクノロジ	選択	2	
	アルゴリズム基礎	選択	2	
	数論基礎	選択	2	
	セキュア法制と情報倫理	選択	2	
	セキュリティ管理と経営	選択	2	
	プレゼンテーション技法	選択	2	
	情報セキュリティ輪講Ⅰ	必須	2	

	授業科目名	履修区分	単位数	修了に必要な単位数
	研究指導	必須	6	6

	授業科目名	履修区分	単位数	修了に必要な単位数
専門	計算代数	選択	2	16
	暗号理論と電子認証	選択	2	
	暗号プロトコル	選択	2	
	個人識別と個人情報保護	選択	1	
	情報システム構成論	選択	2	
	オペレーティングシステム	選択	2	
	セキュリアシステム構成論	選択	2	
	セキュリアシステム実習	選択	2	
	ソフトウェア構成論	選択	2	
	セキュリアプログラミングとセキュリアＯＳ	選択	2	
	不正アクセス技法	選択	2	
	ネットワークシステム設計・運用管理	選択	2	
	セキュリティシステム監査	選択	2	
	情報セキュリティマネジメントシステム	選択	2	
	セキュリティの法律実務	選択	2	
	セキュア社会制度論	選択	4	
	情報セキュリティ輪講Ⅱ	選択	2	
	情報セキュリティ特論	必須	2	

■ 修了要件

以下の3つの条件を全て満たすこと

- 修業年限：２年以上
- 所要単位：３０単位以上
  - 専門基礎科目 ８単位以上（含必修２単位）
  - 専門科目 １６単位以上（含必修２単位）
  - 研究指導 ６単位
- 修士論文など
  - 修士論文または課題研究

Katsuya Uchida uchidak@gol.com

ありがとうございました

情報セキュリティ大学院大学 兼
中央大学 研究開発機構
助教授　内田　勝也
uchidak@gol.com
http://www2.gol.com/users/uchidak/