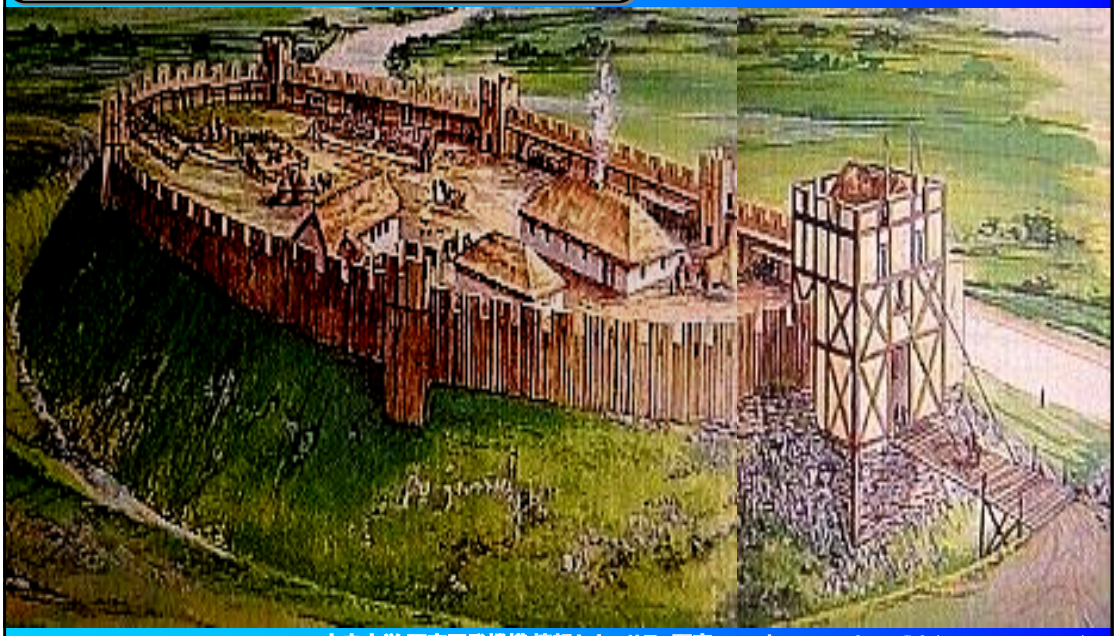
中央大学における
情報セキュリティ・情報保証 人材育成

2003年10月24日
先端技術・情報犯罪とセキュリティ研究会
日本セキュリティ・マネジメント学会



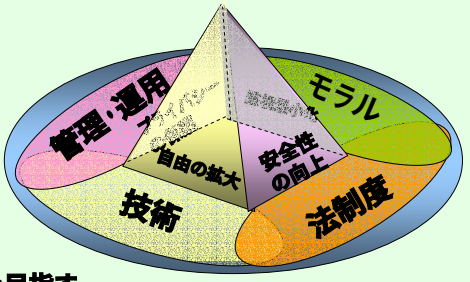
中央大学 研究開発機構 情報セキュリティ研究ユニット　内田　勝也（uchidak@gol.com）

情報セキュリティ 人材育成の必要性

人材育成の背景

- e-Japan計画を始め、安全で信頼できる電子社会を推進するためのセキュリティ技術者・管理者の育成が喫緊の課題である。
- 国内では大学・大学院で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。
- 情報セキュリティは総合科学であり、
  - 技術
  - 管理・運用
  - モラル (倫理)
  - 法制度

  を基礎に置いて、
  情報セキュリティ要員の育成を図ることが重要。

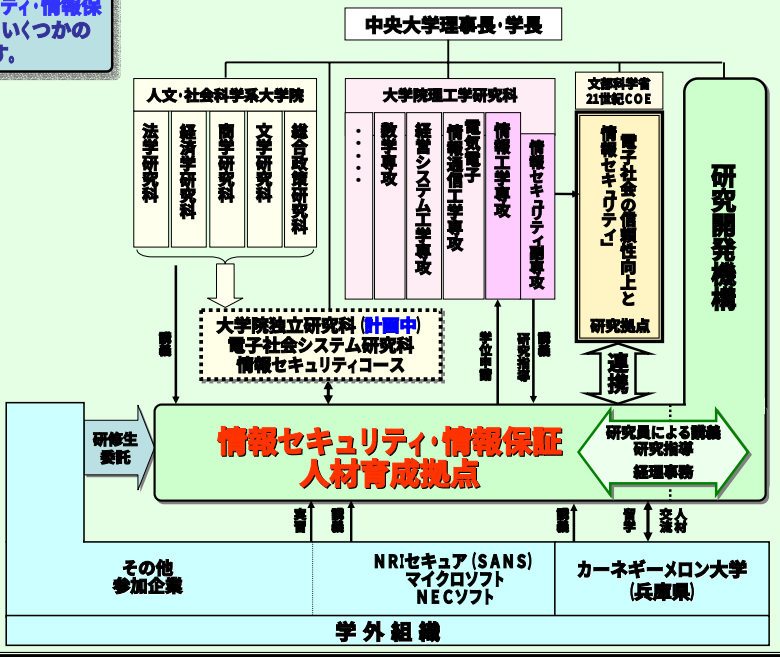


- また、総合的な指導を理論と実践の両面からの育成を目指す。
- 国内では、一部の大学での取り組みが始まっているが、要員育成従事者の不足は深刻。
- 米国では80年代末から、情報セキュリティ教育が大学・大学院で始まっており、国防総省や全米科学財団等の支援を受けた短期の情報セキュリティ教育も行われている。

Katsuya Uchida uchidak@gol.com

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があり、その俯瞰図が右図です。



Katsuya Uchida uchidak@gol.com

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。
- 副専攻は、「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」、「情報セキュリティ」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した。
- 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）を取得すること。

Katsuya Uchida　uchidak@gol.com

中央大学における
情報セキュリティ・情報保証 人材育成

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	講　師
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	辻井重男教授 土井洋 機構助教授
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	越晋輝 教授
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	土屋敏久 教授 内田勝也 機構助教授
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、個別性監査、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	大井正浩客員教授 (駒澤大学教授)
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	安富潔 客員教授 (慶應義塾大学 教授)
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	各講師
	2	半		必	

Katsuya Uchida　uchidak@gol.com

ネットワークセキュリティの講義内容

	講義内容 （火曜日 17:30～19:00）		講義内容 （火曜日 17:30～19:00）
第 1回 4月15日	オリエンテーション セキュリティの概要	第 7回 6月10日	ISMS、ISO15048、OCEDセキュリティガイドライン、セキュリティ監査
第 2回 4月22日	攻撃の種類 情報セキュリティサービス	第 8回 6月17日	ハッカー技術
第 3回 5月6日	情報セキュリティのステップ ポリシー	6月24日	休 講
第 4回 5月13日	インターネットの基本設計 情報セキュリティの最適選択手段	第 9回 7月1日	侵入検知
5月20日	休 講	第10回 7月8日	リスク管理
第 5回 5月27日	暗号 情報セキュリティの法的問題	第11回 7月15日	Windowsセキュリティ UNIXセキュリティ
第 6回 6月3日	ファイアウォール 仮想専用線（VPN）		

参考書として、Eric Maiwald「Network Security A Beginner's Guide」Osborne/McGraw-Hill ISBN 0-07-213324-4 の第1版を利用しましたが、最近、2版が出版されました。

Katsuya Uchida uchidak@gol.com

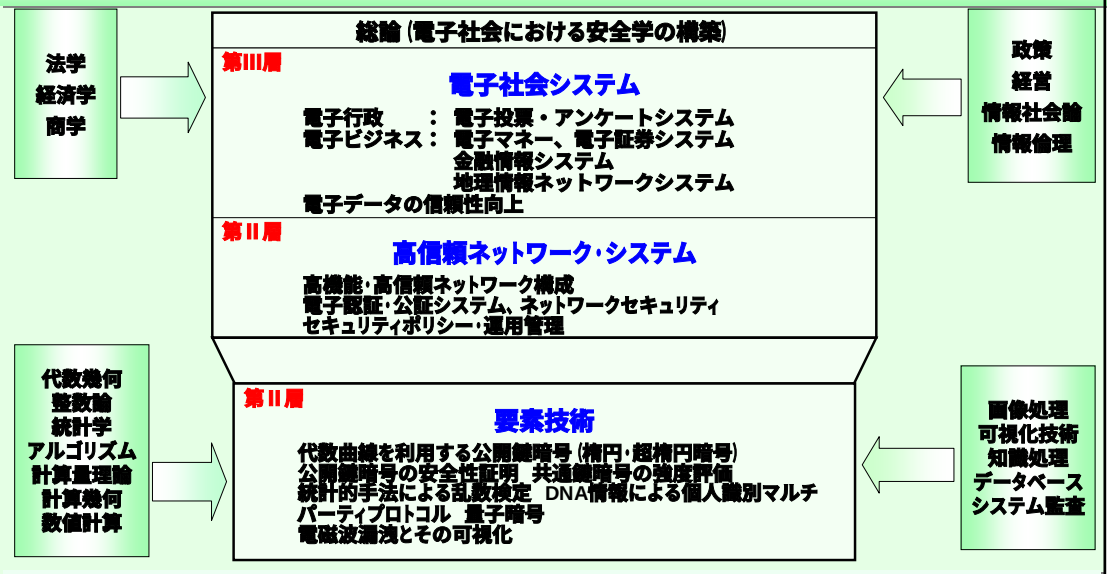
21世紀COEとは？

- 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

人文・社会科学的視点からの助言・評価



情報セキュリティを支える理論と技術

Katsuya Uchida　uchidak@gol.com

中央大学における
情報セキュリティ・情報保証 人材育成

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・情報保証 人材育成

人材育成の背景

- 米国は８０年代後半からセキュリティの重要性が認識され、国防総省がCERT/CCの創設・資金支援等を行ってきた。
- ９０年代後半にサイバー攻撃に対応できる要員の育成支援が大学に対して行われ、現在はNSAが２３大学へ支援を行っており、また、全米科学財団も１３大学に対して支援を行っている。
- 全米の大学院では高度な技術を持った人材の育成が長期間行われており、技術的な面だけでなく、管理・運用面、法律面（証拠保全・法廷対応）の対応や経営層を含め、被害組織へのプレゼンテーションや報告書作成能力を持った人材育成が行われている。
- 日本では、「安全はタダ」との認識が長らく続き、教育機関等においても情報セキュリティの重要性の認識がなく、研究者も非常に少ない。
- 平成１３年度に早稲田大学、大阪大学サイバーメディアセンター等での人材育成が始まっているが、今後必要とする人材の質・量をカバーできる状況ではない。
- また、民間のセキュリティ教育の多くはベンダー依存であり、また体系的な教育が行われていない。基礎的な教育がないため、屋根から家を建てている状況であるとも言える。
- 情報セキュリティに関する専門書籍も少なく、体系的に学ぶことができない状況にある。

Katsuya Uchida uchidak@aol.com

中央大学における
情報セキュリティ・情報保証 人材育成

情報セキュリティ・情報保証 人材育成

パーデュー大学の修士コース

- 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 Web Site　http://www.purdue.edu/

Katsuya Uchida uchidak@aol.com

情報セキュリティ・情報保証 人材育成

講座No	講座名称
CS501	Introduction to Computational Science
CS502	Compiling and Programming Systems
CS503	Operating Systems
CS510	Software Engineering
CS514	Numerical Analysis
CS515	Numerical Linear Algebra
CS520	Computational Methods in Analysis
CS525	Parallel Computing
CS526	Information Security
CS530	Introduction to Scientific Visualization
CS531	Computational Geometry
CS535	Interactive Computer Graphics
CS536	Data Communication and Computer Networks
CS541	Database Systems
CS542	Distributed Database Systems
CS543	Introduction to Simulation and Modeling of Computer Systems
CS544	Simulation and Modeling of Computer Systems
CS555	Cryptography
CS565	Programming Languages
CS569	Introduction to Robotic Systems
CS572	Heuristic Problem-Solving
CS574	Advanced Computer Graphics Applications
CS580	Algorithm Design, Analysis, and Implementation
CS584	Theory of Computation and Computational Complexity
CS586	Algorithmic Robotics
CS590	Topics in Computer Sciences

講座No.	講座名称
CS590B	Topics in Computational Molecular Biology
CS590D	Security Aspects in Distributed Systems
CS590E	Topical Lectures in Information Security
CS590G	Capturing, Modeling, Rendering 3D Structures
CS590M	Geometric Modeling and Graphics (tentative)
CS590N	Embedded Systems Design
CS590R	Unknown Course Title
CS590U	Access Control: Theory and Practice
CS603	Advanced Topics in Distributed Systems
CS614	Numerical Solution of Ordinary Differential Equations
CS615	Numerical Solution of Partial Differential Equations
CS626	Advanced Information Assurance
CS635	Unknown Course Title
CS636	Internetworking
CS638	Multimedia Networking and Operating Systems
CS641	Multimedia Database Systems
CS650	Computational Aspects of Parallel Processing
CS655	Advanced Cryptology
CS661	Formal Compiling Methods
CS662	Pattern Recognition and Decision-Making Processes
CS668	Introduction to Artificial Intelligence
CS690	Seminar on Topics in Computer Sciences
CS690M	Advanced Dynamic Memory Management

表2 パーデュー大学 コンピュータサイエンス修士コース 科目一覧

Katsuya Uchida uchidak@gol.com

Purdue大学でのInformation Security 講座

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

情報セキュリティ・情報保証 人材育成

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@aol.com

中央大学における
情報セキュリティ・情報保証 人材育成

情報セキュリティ・情報保証 人材育成

基本的な考え方

- 「情報セキュリティ・情報保証 人材育成拠点」(リーダー：辻井重男教授)
- 中央大学 研究開発機構の提案、「情報セキュリティ・情報保証 人材育成拠点」(リーダー：辻井重男教授)が平成15年度の文部科学省の科学技術振興調整費・新興分野人材養成 (基盤的ソフトウェア) で採択された。
- 平成15 (2003) 年8月から4年8ヶ月間 (2008年3月まで) 実施する。
  http://www.mext.go.jp/a_menu/kagaku/chousei/
- 「情報セキュリティ 人材育成」では、「情報セキュリティ」は後ろ向き (守り) のものと多くの人が考えるため、「利用者に対する安心感・信頼感」を得るための情報セキュリティを「情報保証 (Information Assurance)」と呼ぶことにした。
- 理論と実践を体系的に行うことが大切であり、中央大学の情報セキュリティ俯瞰図で説明してある他の教育・研究体制と一体になって対応することを想定した。
- 学内 (研究開発機構) で可能なものは学内で行うが、良いものは積極的に外部から導入を図ることを考え、海外 (米国) での教育の導入も考慮した。
- このプロジェクトに正式には記載されていないものでも、関連する情報セキュリティに関する対応も視野に入れた。特に、情報セキュリティ資格試験 (CISSP) など。
- 教育して終わりでなく、教育終了後の人達の組織化も検討しており、人的なネットワークの構築も目指している。

Katsuya Uchida uchidak@aol.com

情報セキュリティ・情報保証 人材育成

5つのカテゴリー

1. 情報セキュリティ実践講座の実施

- 現場で役立つ技術の習得
  - システム管理やセキュリティテストの現場で実際に使われるツール、コマンド、あるいは手法を用いることで、すぐにでも現場で役に立つ技術を身につける。
- 攻撃と防御の双方の観点
  - 単に防御方法を学ぶだけではなく、一般的な攻撃手法や過去に公開されたexploitコードを使った現実の攻撃を実習することにより、脅威の度合いやそのリスクを実感する。
  - また過去の攻撃事例を具体的に教育することで、今後、新たな攻撃手法やシステムの脆弱性に関する調査研究を行う人材を育てることに役立たせる。
- 最新の情報を反映
  - カリキュラムに最新の手法、脆弱性、ツール等の情報を反映させることにより、常に講座を最新の状態に保ち、実用に役立つものとする。
- グループ制による教育
  - 受講者を数名のグループに分け、グループ内でディスカッションを頻繁に行わせることにより、理解を深めるとともに、集団で目的を遂行する能力を養う。
- 座学と実習の融合
  - 座学と実習を取り混ぜて行うことにより、基礎や概念を理解すると同時に、実際の脅威や具体的な設定方法を身をもって体験する。
- 時間的余裕を持ったカリキュラム
  - 確実に理解してもらうために、カリキュラムは時間的に余裕を持ったものとする。
- 修了試験の実施
  - 学習に対するモチベーションを高めるために、筆記および実技による修了試験を実施し、合格者には修了証を授与する。

Katsuya Uchida uchidak@gol.com

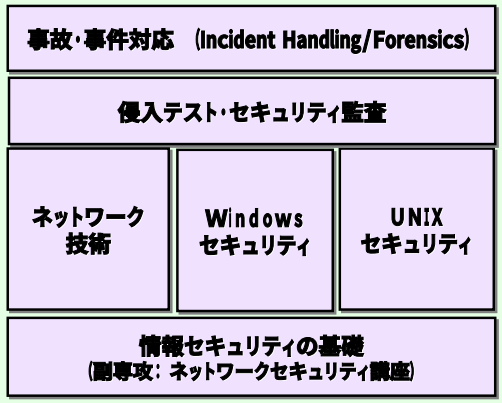
中央大学における
情報セキュリティ・情報保証 人材育成

情報セキュリティ・情報保証 人材育成

1. 情報セキュリティ実践講座の実施 (続き)

今年度の実施計画

- 対象者：情報セキュリティ副専攻履修者、プロジェクトリーダーが適当と認めた者
- 第1回実践講座 (12月13日 [土] ～17日 [水])
  - Windowsセキュリティ実践講座
    - 1日目： Windowsセキュリティの基礎
    - 2日目： Windowsネットワークシステムの脆弱性
    - 3日目： ネットワークアタックとその防御
    - 4日目： ローカルアタックとその防御
    - 5日目： IISセキュリティとIEセキュリティ
- 第2回実践講座 (2月下旬を予定)
  - 1案： 第1回目と同様のものを実施
  - 2案： F/WやIDSを中心とした実践講座
- 第3回実践講座 (可能であれば、3月下旬を予定)
  - 1案： 第1回目と同様のものを実施
  - 2案： F/WやIDSを中心とした実践講座
- 来年度以降は更に充実して実施する予定



Katsuya Uchida uchidak@gol.com

情報セキュリティ・情報保証 人材育成

2．新規講座の開講準備及び開講

- Windowsオペレーティングシステムとセキュリティ講座
  - 大学レベルでWindows ＯＳについての教育が殆ど行われていない。
  - 技術系大学レベルでは、ＭＣＡ資格として、WindowsＯＳがある。
  - 大学院レベルでの利用を想定したカリキュラムの作成を検討し、標準OSの1つとして講座を目指す。
  - 更に高度な研究を希望する場合には、Windowsのソースプログラムを利用した研究も考慮する。
- 情報セキュリティ管理システム講座の開設検討
  - 情報セキュリティ管理システム (ISMS) は、自治体、企業など喫緊のものになっており、ＩＳＭＳに関するカリキュラムの検討を行い、講座として開設することを目指す。
- カーネギーメロン大学 修士コース導入の検討
  - 16ヶ月の修士コースで、技術者向けと管理者向けの2つのコース
    MSISTM (Master of Science in Info. Security Technology & Management) 及び
    MSISPM (Master of Science in IS Policy & Management) の導入を検討。
  - 短期間で体系的にセキュリティ教育の目指す。
  - MSISTM は、情報セキュリティ技術と企業経営・方針に関する包括的な教育を行うことにより、情報セキュリティの指導者育成を目指している。MSISTMは、技術を持った個人で、組織管理・方針を行うことに興味を持っている個人に適している。
  - MSISPM は、管理者や方針決定者として、分析方法や実際の管理業務を通して、セキュリティポリシーの策定やセキュリティ業務管理を修得する。

Katsuya Uchida　uchidak@gol.com

情報セキュリティ・情報保証 人材育成

2.2 カーネギーメロン大学 修士コースの概要

- MSISTM
  - 16ヶ月 (秋・春・夏・秋の4学期) で実施され、管理、技術、セキュリティ及びプロジェクトないしは論文の4つのコア部分からなっている。
  - 管理、技術、セキュリティの3つのコア分野では、それぞれの専門的な能力の確立を目指している。
  - 各コア分野では、以下の講義が行われる
    - 管理分野
      - 情報セキュリティリスク管理
      - 経営経済学と企業経営
    - 技術分野
      以下の内、2つを選択
      - OS (オペレーティングシステム) の設計と実装
      - 通信ネットワーク入門
      - パケットスイッチングとコンピュータネットワーク
      - 分散システム
    - セキュリティ分野
      - コンピュータセキュリティ入門 及び、以下の2つを選択
      - ネットワークセキュリティ
      - セキュアソフトウェア工学
      - 応用暗号学

	秋学期	春学期	夏学期	秋学期
管理分野	経営経済学と企業経営	情報セキュリティリスク管理	プロジェクト／論文	選択
技術分野	以下の1科目選択 ★ 通信ネットワーク入門 ★ パケットスイッチングとコンピュータネットワーク ★ OS (オペレーティングシステム) の設計と実装	分散システム		選択
セキュリティ分野	コンピュータセキュリティ入門	ネットワークセキュリティ		セキュアソフトウェア工学
選択科目	選択	応用暗号学	選択	選択

MSISTMのスケジュール例

  - 更に、学生は科目の選択を工夫することで、関心のある分野の1つないしは2つのテーマに集中したカリキュラムを独自に作成することができる。
  - また、夏学期を実務研修やプロジェクト業務を行うことにより、論文研究を行うことも考えられる。
  - 16ヶ月で修士に必要な課程を修了することが求められるが、プロジェクトを実施するために更に時間が必要なことも考えられ、プロジェクトの遂行に、もう1学期延長することも可能。

Katsuya Uchida　uchidak@gol.com

2.2 カーネギーメロン大学 修士コースの概要 (続き)

- MSISTM
  - 成長が著しく変化の激しい情報セキュリティ分野の管理者に必要な分析的手法や実践的な経営能力を備え、また、情報セキュリティの主要な項目の全般的かつ技術的能力を兼ね備えた学生を育成することを目指しており、MSISTMと同様、16ヶ月での履修を前提としている。
  - 特に、このコースは、CSO (Chief Security Officer: 情報セキュリティ管理者) 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
    - 特定業界における特に重要なセキュリティポリシーに対する理解と対応
    - 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家としての成長を自分自身に課すことができること
  - 最初の2学期間は、効果的なセキュリティ管理やポリシー分析に必要な基礎的な講座を実施する。大部分の授業は技術、分析、定量的ツール、コミュニケーション、管理技術等の中核的なコースとなる。
  - 後半の2学期では、セキュリティ技術や実際的な経営管理分野を更に深く行う。
  - このコースの期間を通して、情報セキュリティにおける特別な課題に特化した選択を行うこともできる。

Katsuya Uchida uchidak@aol.com

中央大学における
情報セキュリティ・情報保証 人材育成
情報セキュリティ・情報保証 人材育成

必修科目	72単位
財務モデル	6
組織管理と情報セキュリティ	12
情報セキュリティ管理入門	12
情報セキュリティ経済学	6
不確実下での意思決定	6
IT管理者のための統計学	6
セキュリティポリシーセミナー：ヘルスケア、金融、政府機関 (2科目選択)	12
コンピュータ・通信セキュリティ入門	12
セキュリティ科目の選択 (3科目選択)	36単位
セキュリティアークテクチャーと分析	12
通信セキュリティ	12
情報セキュリティの先端的な話題	12
情報セキュリティリスク管理	12
一般科目選択	36単位
プロジェクトまたはインターシップと論文 (1科目選択)	36単位
情報セキュリティプロジェクト	36
論文	36
単位の合計	180単位

MSISPMのカリキュラム

Katsuya Uchida uchidak@aol.com

情報セキュリティ・情報保証 人材育成

3．SANS講座（オープンカレッジ）の開講

- 実践的な情報セキュリティ教育として、広範囲をカバーしており、内容としては定評があった。
  （2000年秋に米国で教育コースに参加した経験も参考になった。CSI Conferenceとは別の面での良さがあった。）
- 各コースは、5日ないし6日間行うもので、
- 単に教育を行うだけでなく、資格試験（GIAC：Global Information Assurance Certification）があり、客観的に技術・スキルを証明できる仕組みになっている。
- また、GIACは継続教育を行わないと資格が消滅するようになっており、技術・スキル維持が必要な仕組み。
- 国内ではNRIセキュア社が開講を考えており、日本人講師による対応も考えていた。
- SANSが実施している教育コースには以下のものがある。（青文字は2003年9月に実施）
  - Track 1： SANS Security Essentials Bootcamp and the CISSP 10 Domains
  - Track 2： Firewalls, Perimeter Protection and VPNs
  - Track 3： Intrusion Detection In-Depth
  - Track 4： Hacker Techniques, Exploits and Incident Handling
  - Track 5： Securing Windows
  - Track 6： Securing Unix
  - Track 7： Auditing Networks, Perimeters and Systems
  - Track 8： System Forensics, Investigations, and Response
  - Track 9： Security +STM
  - Track 11： SANS 17799 Security and Audit Framework
  - Track 12： SANS Security Leadership Essentials for Managers

Katsuya Uchida uchidak@gol.com

中央大学における
情報セキュリティ・情報保証 人材育成

情報セキュリティ・情報保証 人材育成

3．SANS講座（オープンカレッジ）の開講（続き）

SANS Security Essentials Bootcamp and the CISSP 10 Domainsの内容（6日間）

- SANSのセキュリティ概論Ⅰ：ネットワークの概念
  ネットワークやTCP/IPのようなプロトコルなどがどのように動作するのかを知ることは、ネットワークトラフィックの解析や悪意のあるトラフィックを特定するために非常に重要です。また、ルーターやファイヤーウォールのようなネットワーク関連機器を使ってセキュリティを確保することも同様に重要なことです。ここでは、効果的にアタックを阻止する対策と、それらアタックをタイミングよく見つける手段にについて学ぶ。
- SANSセキュリティ概論Ⅱ：ネットワークセキュリティの概観
  ネットワークセキュリティにおける6つの重要な内容について学ぶ。まず、情報セキュリティの脅威を理解し、それがどのように機密性（Confidencality）、完全性（Integrity）、可用性（Availability）に影響を及ぼすか、また、健全なセキュリティポリシー、UnixとWindowsそれぞれのパスワード管理、アクセスコントロール、情報戦争の脅威とインシデントハンドリングについて解説する。
- SANSセキュリティ概論Ⅲ：インターネットセキュリティテクノロジー
  侵入検知システムやファイヤーウォールなどの様々なセキュリティ機器の導入を検討している企業が具体的なアクションがとれることが目的です。企業内に介在する全ての問題を解決するために、何層もの防御策を講じるといった綿密な防御戦術をとるなど、情報セキュリティ施策を確立するヒントを与える。
- SANSセキュリティ概論Ⅳ：セキュリティコミュニケーション
  情報セキュリティにとって有効な手段に情報の暗号化がある。 暗号化に関する様々な局面と、企業の情報資産を保護する上でどのように使用すべきかとを取り扱い、暗号化によって防ぐことのできる各種攻撃についても考察する。また、現在出回っている膨大な数のウィルスと、企業への影響を考察し、ウィルスとウィルス検知に関しても解説する。
- SANSセキュリティ概論Ⅴ：Windows Security
  Windowsは、全世界で最も使われており、最も攻撃頻度の高いOSで、更に、Windows 2000、Windows XP、Windows .NET Server、そして Active Directory といった製品は、今後のWindowsの状況を一変させようとしている。ここでは、情報セキュリティの観点からMicrosoftの次世代技術の進化をいち早く学習し、単純化、自動化可能なツールについて解説する。これによって、Windows 2000/XP/.NET のセキュリティに関して、確かな知識を身につけることができる。
- SANSセキュリティ概論Ⅵ：Unix Security
  業界の共通認識となっている標準に基づいて、ここでは、いかなるUNIX OSのセキュリティをも向上させるためのガイダンスを提供する。UNIX入門者向けに基礎的な情報を講義しながら、「最適な実施方法」をアドバイスします。

Katsuya Uchida uchidak@gol.com

3．SANS講座（オープンカレッジ）の開講（続き）

Firewalls, Perimeter Protection and VPNs の内容（6日間）

- IP Stimulus/Response and Fragmentation
- Complex IP Transports and Services
- TCPdump, WINdump, Ethereal and Other Sniffers
- Business Needs vs. Security
- Static Packet Filtering
- Stateful Packet Filtering and Inspection
- Proxies
- In-depth Coverage of Popular Firewall Products
- Implementing Security with Cisco Routers Intrusion Detection
- Centralized Logging
- Firewall Log File Analysis
- Log File Alerting
- IPSec, SSL, and SSH
- Designing a Secure Perimeter
- "Cool Tools“
- Network and Host Based Auditing

Katsuya Uchida uchidak@aol.com

中央大学における
情報セキュリティ・情報保証 人材育成
情報セキュリティ・情報保証 人材育成

3．SANS講座（オープンカレッジ）の開講（続き）

Intrusion Detection In-Depth の内容（6日間）

- TCP/IP for Intrusion Detection
  - TCPdump Review
  - TCP/IP Communication Model
  - Fragmentation
  - ICMP
  - Stimulus and Response
  - Microsoft Networking and Security
  - Domain Name System
  - Routing
  - IPsec
- Network Traffic Analysis Using tcpdump
  - Introduction to TCPdump
  - Writing TCPdump Filters
  - TCPdump Filters
  - Analysis of TCPdump Output
  - Advanced Analysis
  - Examining Datagram Fields with TCPdump
- Intrusion Detection Using Snort
  - Introduction
  - Modes of Operation
  - Writing Snort Rules
  - Configuring Snort as an IDS
  - Output Analysis
  - Advanced Topics
- IDS Signatures and Analysis
  - Intrusion Detection Architecture
  - A Close Look at the Famous Mitnick Attack
  - Intrusion Detection Analysis
  - Common Errors and How to Avoid Them
  - Traffic and Externals Analysis

Katsuya Uchida uchidak@aol.com

3．SANS講座（オープンカレッジ）の開講（続き）

Hacker Techniques, Exploits and Incident Handling の内容（5日間）

- Incident Handling Step-by-Step Computer Crime Investigation
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Special Actions for Responding to Different Types of Incidents
  - Incident Record Keeping
  - Incident Follow-Up
- Computer and Network Hacker Exploits
  - Reconnaissance
  - Scanning
  - Intrusion Detection System Evasion
  - Network-Level Attacks
  - Gathering and Parsing Packets
  - DNS Injection
  - Operating System and Application-Level Attacks
  - Web Application Attacks
  - Denial of Service Attacks
  - Maintaining Access
  - Covering the Tracks
  - Putting It All Together
- Hacker Tools Workshop
  - Hands-on Installation and Analysis
  - General Exploits
  - Other Attack Tools and Techniques

Katsuya Uchida uchidak@aol.com

中央大学における
情報セキュリティ・情報保証 人材育成
情報セキュリティ・情報保証 人材育成

3．SANS講座（オープンカレッジ）の開講（続き）

Auditing Networks, Perimeters and Systems の内容（6日間）

- Auditing Principles and Concepts
  - Auditor's Role in Relation to
  - Benefits of Various Auditing Standards and Certifications
  - Basic Auditing and Assessing Strategies
  - The Six-Step Audit Process
- Auditing the Perimeter
  - Overview
  - Detailed Audit of a Router
  - Testing the Firewall
  - Testing the Firewall Rulebase
  - Testing Third Party Software
  - Reviewing Logs and Alerts
  - The Tools Used
  - War Dialing
  - War Driving
- Auditing Web Based Applications - Hands-on
- Auditing Networks with Nmap and Other Tools - Hands-on
  - Introduction
  - Getting Started With Nmap
  - Mapping Your Network
  - Analyzing The Results
  - Follow-on Activities
- Advanced Systems Audit: Windows NT/2000 - Hands-on
  - Auditing to Create a Secure Configuration
  - Auditing to Maintain a Secure Configuration
  - Auditing to Determine What Went Wrong
  - Forensics
- Advanced Systems Audit: Unix - Hands-on
  - Auditing to Create a Secure Configuration
  - Auditing to Maintain a Secure Configuration
  - Auditing to Determine What Went Wrong
  - Forensics

Katsuya Uchida uchidak@aol.com

3．SANS講座（オープンカレッジ）の開講（続き）

System Forensics, Investigations, and Response の内容（6日間）

- Forensic and Investigative Essentials - Hands-on
  - ◆Incident Response and Forensics
  - ◆Forensic Theory on Any Operating Systems
  - ◆Hands-On Forensic Lab Configuration
- Basic Forensic Principles Illustrated with Linux - Hands On
  - ◆Essential Forensic Tools
  - ◆How to Collect and Protect Evidence - The Disk Image
  - ◆Heart of the Crime in Linux
  - ◆Filesystem Forensics
  - ◆Network Forensics
  - ◆Analyzing a Real World Compromise
- The Coroner's Toolkit, TASK, and Autopsy - Hands-On
  - ◆ TCT Toolkit
  - ◆ TASK Toolkit
  - ◆ Creating Timelines
  - ◆ Autopsy Forensic Browser
- Windows 2000/XP Forensics - Hands-On
  - ◆ Windows Live System Examination
  - ◆ Windows 2000 Imaging
  - ◆ Searching for clues
  - ◆ Registry and Information
  - ◆ Malicious Programs
  - ◆ Low-Level Analysis
- Frameworks and Best Practices: Managerial and Legal Issues
  - ◆ A Framework for Forensics Concepts
  - ◆ Legal Permissions and Restrictions on Internal Investigations of Incidents
  - ◆ Internet Service Providers
  - ◆ Law Enforcement
  - ◆ Evidence Integrity
- Advanced Forensic - Hands-on
  - ◆ Kernel Module Forensics
  - ◆ Malware Dissection and Analysis
  - ◆ Advanced /proc directory breakdown
  - ◆ Process Wiretapping
- The Forensic Challenge
  - ◆ The Forensic Challenge

Katsuya Uchida uchidak@gol.com

中央大学における
情報セキュリティ・情報保証 人材育成
情報セキュリティ・情報保証 人材育成

4．脆弱性データベース構築を通した高度技術者の育成

- ネットワークセキュリティ上の問題の解決のために必要なセキュリティホール情報の多くは海外からの情報の頼っているのが現状であり、次の問題が顕在化しつつある。
  - ◆ 一般ユーザが家庭、職場で活用するのが難しい
  - ◆ 現在はJPCERTや外資系企業等のサポートを利用できるが、基本的に海外のソフトのみ対応である。
  - ◆ 我国のメーカー、ベンダーの脆弱性データベースは存在するが、利用しにくい(個々に存在しているが、統一が取れていないのが状況である。
  - ◆ 我国の企業(海外支店等)で活用可能なものが少ない
- このような現状を踏まえ、本サブテーマでは、脆弱性プログラムの調査･解析は、最も高度なセキュリティ技術の1つであることを思量し、脆弱性データベースの構築を通して、高度技術者の育成を行う。
- 大学という中立な立場から、データの収集を行うため、一般企業に比べ容易に収集可能であり、また、脆弱性データベース構築を実現し、国際的かつ統一の取れた標準的なインタフェースを提供し、e-Japanや電子社会の進展に寄与することも可能となる。

Katsuya Uchida uchidak@gol.com

情報セキュリティ・情報保証 人材育成

5．中央大学独立研究科電子社会システム研究科 情報セキュリティコースの開講

- 21世紀の電子社会に対応するため、総合大学としての中央大学の特徴を十分生かした文理融合型の新たな研究科における情報セキュリティコースでの開講に耐え得る、高度な人材育成を目的としたカリキュラムの調査研究、実現、評価を目標とする。
- 情報セキュリティコース
  - 法制度(電子署名法、個人情報保護等)の研究
  - 管理運用(セキュリティポリシー、セキュリティ評価基準、システム監査等)の研究
  - セキュリティ技術(ネットワークセキュリティ、個人識別、暗号技術等)の研究

- **オープンカレッジの実施　2003年12月19日(金)～23日(水・祝)　詳細は別途**
  - 21世紀COEとの協同でシンポジウム、特別研修コースを実施する。(後楽園キャンパス、無料)
  - シンポジウム：　情報セキュリティにおける研究・人材育成拠点形成へ向けて
    - 19日(金)　10:00～17:00　各研究グループ代表者による成果発表
    - 20日(土)　10:00～12:00　パネル(学内教授・研究者)
      13:00～15:00　パネル(外部アドバイザー)
      15:30～16:30　特別講演　木村 剛 氏 KFI代表取締役
      16:30～19:00　懇親会
  - 特別研修コース「電子社会システムと情報セキュリティ」
    - 21日(日)・22日(月)・23日(火・祝)　09:30～18:10
    - 特別講演：　白川秀樹博士
    - 学内外の方々による1時間の講座(20講座程度)
    - 7割以上の出席者には、終了証書を発行

ありがとうございました

ご質問・コメントがございましたら ・・・・

中央大学 研究開発機構
情報セキュリティ研究ユニット
助教授　内田　勝也
uchidak@gol.com
http://www2.gol.com/users/uchidak/