セキュリティ技術者養成センター

計画の目標・概要

１．目標
（１）セキュリティ教育の標準カリキュラムの策定（13 年度末）。
（２）（１）に基づく講義によるセキュリティ技術者（学士／修士レベル）の育成（14 年度―17 年度。60 人／年程度以上を目標）。
（３）（１）に基づく Web Based Training（WBT 遠隔教育）電子化教材作成および本教材によるインターネット遠隔授業オープン提供（14 年度末以降。数百人／年以上の学外利用を想定）。
（４）企業との連携講座による博士レベルのセキュリティ研究者育成ならびに世界レベル研究成果の輩出（16 年度―17 年度。4―5 人／年程度を目標）。
２．内容
（１）標準カリキュラム策定には企業技術者の協力を得る。
（２）企業技術者および研究者の協力による講義の受講を通じて知識の獲得。
（３）企業との連携講座における一流研究者の指導による研究環境。
（４）海外研究者の招聘研究。

諸外国の現状等

１．現状
Clinton大統領の時代から国家安全の観点でセキュリティ対策が論じられ、これを受けてUniv. of California(Davis)のComputer Security Lab.やPurdue大学のCOASTプロジェクトなどにおいて、セキュリティ研究およびセキュリティ教育プロジェクトが進んでいる。
２．我が国の状況
セキュリティ教育および研究の重要性は総合科学技術会議などで十分に認識されているものの、そのための技術者・研究者育成策については今後の課題とされている。ただし、今後のe―Japan計画などの推進のために相当数の技術者・研究者は必要。

計画進展・成果がもたらす利点

電子商取引・電子化政府などのような、今後の国家的IT戦略推進のための基本的な人材提供が可能となる。ネットワーク・テロ対策の基本技術開発力を有する研究者育成ができ、安全かつ先進的なIT国家構築に寄与できることになる。
また標準カリキュラム策定ならびにインターネット教材作成により、早稲田大学のみならず、日本全体としてのレベル向上にも資することができる。
さらに、企業との連携講座によりこれを進めることにより、現在IT分野において強く要求されている、「産官学を含めた実用化指向技術ポテンシャル」向上を可能とする。

セキュリティ技術者養成センター

1．目標

（1）直接的な目標

・セキュリティ技術者（学士・修士レベル）の育成

ー早稲田大学から、６０人／年。学外から（遠隔授業）、数百人／年

・セキュリティ研究者（博士レベル）の育成

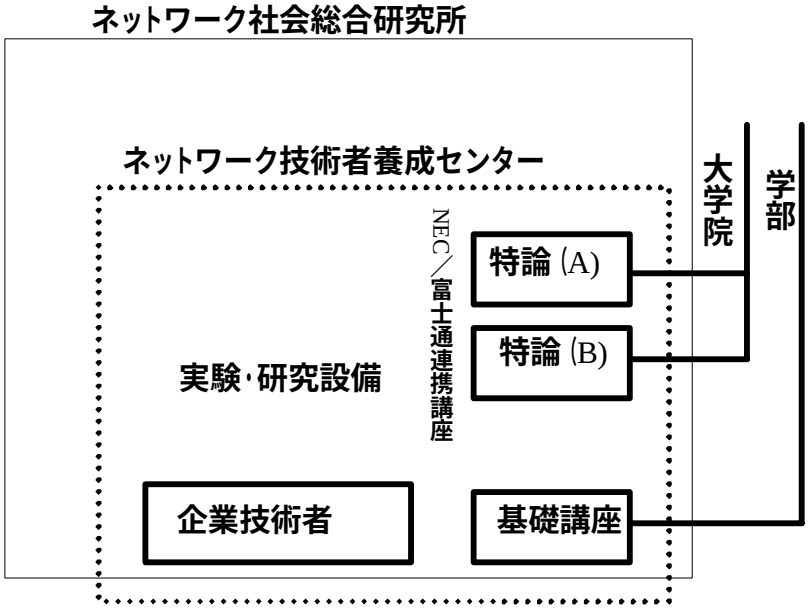
ー４ー５人／年

（2）間接的な目標

・セキュリティ教育標準カリキュラム作成ならびに電子化教材（遠隔授業も可能）の作成

・セキュリティ実証実験などのための企業・大学共同利用設備（センター）の開設

2．体制（早稲田大学理工学部内）



（1）産業界の協力

・後藤敏氏（日本電気）、林弘氏（富士通研究所）

ー客員教授（予定）として連携講座を担当

ー大学院学生などの研究指導。各機関などにて実施を委託

・NPO ネットワークリスクマネジメント協会

ーカリキュラム作成、電子化教材作成、実証実験など

（2）早稲田大学メンバー ー セキュリティおよび関連する社会的活動

・中島　達夫　ーセキュァ OS・組み込み Linux コンソーシアム代表

・後藤　滋樹　ーセキュァ NW・JPNIC、APAN などの理事など

・村岡　洋一　ーセキュァな AP・Grid Forum Advisor

3．想定される研究テーマ

セキュリティ製品の評価、Confirmance test、不正アクセス検出、振る舞いに基づく検出、セキュリティホール対策、ユビキタス環境における携帯機器の高信頼化(経済性・簡便性)セキュリティ推奨案の作成など

人材養成計画の趣旨・概要

【人材養成計画の趣旨】

電子化政府計画の進展、また最近のテロ事件の発生などを見るまでもなく、セキュリティ教育および研究の重要性は、総合科学技術会議などで十分に認識されており、今後のe－Japan計画などの推進のために相当数の技術者・研究者が必要であることが指摘されている。したがって、そのための技術者・研究者育成策はこれからの最重要課題の一つである。
現状では、セキュリティ技術については、暗号などの理論的な分野の研究・教育は大学でも活発になされているものの、本当に必要とされているのは現実のソフトウェア・ハードウェア。ネットワークなどに即した実戦的な技術に関する体系的教育ならびに研究である。しかしこれらの事項に関するノウハウの大半は企業にあり、全く現場での担当者レベルの知識としてしか行かされていないのが現状である。このような状況を打破して、それらのノウハウの学問としての体系化、それを元にした体系的教育を施された学生の輩出、ならびにそれに基づいた抜本的に新しいセキュリティ技術の研究・開発をすすめる。

【人材養成計画の概要】

（1）企業との協力により、体系的なセキュリティ技術教育のための標準的カリキュラムの策定。
（2）企業のセキュリティ技術者が参加する人材養成講座を設けて、実際的な知識・技術の習得を可能とすることにより、一流の学士／修士レベルのセキュリティ技術者育成をはかる。
（3）企業と協力して、企業研究者によるセキュリティ講座ならびに研究指導など、一流セキュリティ技術者・研究者とのチーム研究に大学院学生を参加させることにより、一流の博士レベルの研究者を育成する。この実施に当たっては、国外の一流研究者を短期招聘し、共同研究の機会を設けることにより、さらに一流の成果をあげる。
（5）（1）に基づく電子化教材を作成し、これをインターネットで公開、インターネット授業として提供することにより、学外の技術者教育にも参画。

育成目標は以下のようである。

・セキュリティ技術者（学士・修士レベル）の育成
　　－早稲田大学から、６０人／年。学外から（遠隔授業）、数百人／年
・セキュリティ研究者（博士レベル）の育成
　　－４－５人／年

【人材養成ユニットの実施体制】

項　　目	担当機関	担当者
１．養成業務従事予定者の招聘	学内学生を対象	情報学科事務所
２．養成対象者の選考	一般の科目受講であるので、特に選考はない。	
３．講義・研究開発		
（１） ネットワークセキュリティ基礎 （学部学生）	情報学科設置	◎村岡他
（２） 情報セキュリティ特論（A） （大学院学生）	同上	後藤敏教授
（３） 同上（B）	同上	林弘客員教授
（４） 遠隔授業 （学外生：来年度から実施の計画）	同上	村岡他

（注：全体計画の代表者には◎を付す）

【所要経費一覧（平成１３年度、１４年度は決算額、平成１５年度は予算額を記入）】

平成１３年度	平成１４年度	平成１５年度
４９百万円	４９百万円	４７百万円

【所要経費の内訳（平成１３年度、１４年度は決算額、１５年度は予算額を記入）】

（単位：百万円）

	１３年度	１４年度	１５年度
調整費充当計画			
１．人件費	3	3	2
（１） 客員教授	1	1	1
（非常勤扱い）	（2名）	（2名）	（1名）
（２）嘱託	3	2	2
	（１２名）	（２７名）	（２６名）
２．試験研究費	３５	４０	１３
（１）機械装置	３１	３２	9
（２）賃金	4	8	4
（主なものを記入）			
３．旅費	1	1	1
（１）試験研究旅費	0	0	0
（２）外来研究員等旅費	0	0	0
（３）外国旅費	1	1	1

４．その他 （1）国際シンポ開催 （2）遠隔授業環境構築	0 0 0	0 0 0	9 0 9
計	４０	４４	２５

成果の概要

【人材養成計画の進捗状況】

①人材養成講座の設置

人材養成講座として、大学院レベル（2 講座）および学部レベルの授業を開設し、学生の指導を行った。

具体的には、以下の３講座を開講した。

(a) ネットワークセキュリティ基礎（学部４年生対象） 後期半期

情報セキュリティに関する基本的な知識の習得を目標とした。セキュリティについては、特に社会的な関係（意義、規則など）に関する知識の涵養が不可欠なので、その点に特に配慮した。

- 情報セキュリティとは
- 個人情報保護法と不正アクセス防止法
- 暗号化技術
- ネットワーク高信頼化技術
- ウィルスとは
- ファイァウォール技術
- その他
- 実験・実習： ウィルス検知、ファイァウォール設定、ログ解析など

(b) 情報セキュリティ特論（A）（大学院修士学生対象） 後期半期

本講座では、主にセキュリティの技術専門家の育成を目標とした。現在のセキュリティ技術最先端の状況の理解とそれらの弱点の把握、さらにそれらについての対策などを実践的に学ぶ環境を提供した。

(c) 情報セキュリティ特論（B）（大学院修士学生対象） 後期半期

本講座では、主にセキュリティの法律的、社会的側面に力点をおいて、技術者として学ぶ環境を提供した。利用者としてもどれだけのことをしておかないとネットワーク社会での責任をはたすことができなくなるか、また現在の法体制の限界などについても理解できるように配慮した。

② 標準的カリキュラムの策定・検討

昨年度作成したカリキュラムを元に、今年度行った授業の経験や社会的環境の変化さらには技術的進歩などを勘案した改編を行った。

主要な変更点は、以下のようである。

（1） セキュリティは最終的には「人」の倫理観などを含めた育成である点を重視し、インターネットでなぜ「悪いこと」を人はやりやすいと感じているのか、ということにつき、種々の観点からの考察を加えることとした。
（2） 反面、学生の技術的な興味に応えるために、最新の研究成果（例：スタックオーバフローへの対策）などの実例を強化した。

このカリキュラムによる特別講義（前１３回。集中）を琉球大学学部生を対象に実施し、カリキュラムの一般性を検証した。

上記に基づき、カリキュラム検討報告書を作成した。

③インターネット授業

電子化の前段階として、昨年度収集した教材原稿作成のための必要な情報をもとに、CD-ROM 化したオンライン教材を作成した。あわせて、インターネット授業のためのシステム構築を行なった。

具体的な内容は以下のようである。

（1） 教材ＣＤ－ＲＯＭ作成。
この配布については、著作権などの問題の確認を現在実施中である。
（2） 遠隔講義システム
Ｗｅｂベースで上記の教材を閲覧するとともに、質問その他を適宜行えるような仕組みを組み入れたシステムを構築した。上記と同じく著作権の問題の解決があるので、現時点では学内のみの開放である。

以上について、それぞれＣＤ－ＲＯＭ作成および付随する説明書を作成した。

【目標に対する達成度】
：当初目標（３年目の目標）に対する目標の達成度を記載してください

養成する人材のレベル	実績（目標）
・学部学生（13 年度） ・同上（14 年度） ・同上（15 年度） ・博士（13 年度） ・同上（14 年度） ・同上（15 年度）	55 人（60 人） 70 人（60 人） 80 人（60 人） 0 人（4 人） 2 人（4 人） 3 人（4 人）

１５年度ユニット所属者数 （うち１５年度終了見込み数）
左記参照

（実績は１５年度までに当該課程を終了または終了見込みの者を記載）

【養成された人材の概要】

（1） 技術者・研究者としての可能性
これまでの育成過程において、例えば以下のように素晴らしい研究成果をあげられる学生が輩出している。

(a) ユビキタス環境におけるプライバシィの保護
オフィス環境での機密保護を狙って、単なる入居者の情報機器の使用履歴のみならず、物理的な色々な動作の履歴を保管して、これを基にセキュリティを担保する仕組みを提案した。
(b) セキュァなメーリングシステム
電子メールにおけるメーリングシステムの問題は、購読者以外に対する秘密保持の実現にある。この研究では、管理者による「盗み見」なども防げるようにするために、これまでの公開鍵方式をさらに発展させた新しい暗号方式を提案した。
(c) スタックオーバフローの防御
最近のウィルスなどにおける最大の課題であるスタックオーバフローに対応るためにコンパイラおよびC 標準ライブラリの置き換えによる対策を提案した。この手法はIBM やNTT などの企業で高く評価された。
(d) ルータベーストレースバック手法の提案
DoS 攻撃など、セキュリティに対する攻撃があった場合、それがどこから来たのかを検知するために、既存ルータには最小限の修正を加えるのみでいい、新しい攻撃経路検知手法を提案した。
(e) システムコール分析による攻撃検知手法
不正アクセスを検知するために、平常時のプロファイルを生成して、これに対する変位を解析する手法を提案した。
(f) ソフトウェア利用認証方式
ソフトウェアの不正使用を防護するために、ネットワークを介してソフトウェアを配布するとともに、その使用を公開鍵を使用して認証するシステムを提案した。

以上の成果については、それぞれ学会などにおいて報告され高く評価されている。

（2） 企業における活躍

・NTT、IBM などの企業の研究所においてセキュリティ対策の研究員として活躍する学生が増えた。
・企業において電子政府を実現する部門で活躍する学生が増えた。

（3）v-staff

セキュリティ分野で現在最大の課題は、セキュリティを脅かすような兆候を如何に迅速に検出して、これを適切に関係者に通知するかということである。これは、天気予報における、台風予報などに比較すればその重要性が分かるはずである。このような「予報システム」の重要性はアメリカなどでは早くから認識され、いわゆる CERT システムとして実現され。サービスが一般に提供されている。これに対して日本ではその重要性は認識されているものの、実現は大きく遅れていた。これに対して、本プロジェクトによって育成された学生が自発的に、セキュリティのアラート情報の構築を始め、現在で v-staff として、サービス提供に至っている。

v-staff の活動は，システムのセキュリティホールに関する日本語データベースを構築し、広く無料で提供することにより、日本のセキュリティ対策の向上に貢献することを目的としている。現在はその第一歩として，ISS 社の協力の元、X-Force DB を日本語ローカライズした脆弱性 DB の構築を行っている。

NPO 法人であるネットワークセキュリティ協会 NRA などとの産学連携した取組みとして開始し、早稲田大学の学生有志とネットワークセキュリティに関連する企業の有志がボランティアメンバとして集まり活動を行っている。

現在は日本語によるシステムの脆弱性に関する情報を整理・蓄積し、ユーザに幅広く提供していくことが日本におけるネットワーク危機の発生防止，危機発生時の迅速な対応に大きく役立つと考え、日本語による脆弱性 DB を構築し無償で公開する活動を進めている。

本システムは、現在２０００を越える情報を有しており、最終的には電子政府の各拠点にセキュリティに対する脅威情報を確実かつ迅速に伝えることができるボランティアサービスとすることを目指している。

このようなボランティア活動によってセキュリティ実現を目指す学生が着実に増えている。

（3） その他

本学の学生に加えて、前記の講義の内容を外部にも提供している。具体的には、琉球大学における特別講義、各自治体における講演会などを通じて、現場で電子政府の開発・運営を担当している職員などへの啓蒙活動を行ってきた。

これらの卒業生の中には、すでに企業の研究所でセキュリティ技術者として頭角を表しているものも出現しており、将来の電子政府の安全性を確保するに重要な人材となることは確実である。

【想定外の成果、困難について】

特に無し。