

パネルディスカッション
ICTシステム運用の未来

セキュリティを含めた人材の育成

早稲田大学 基幹理工学部

情報理工学科

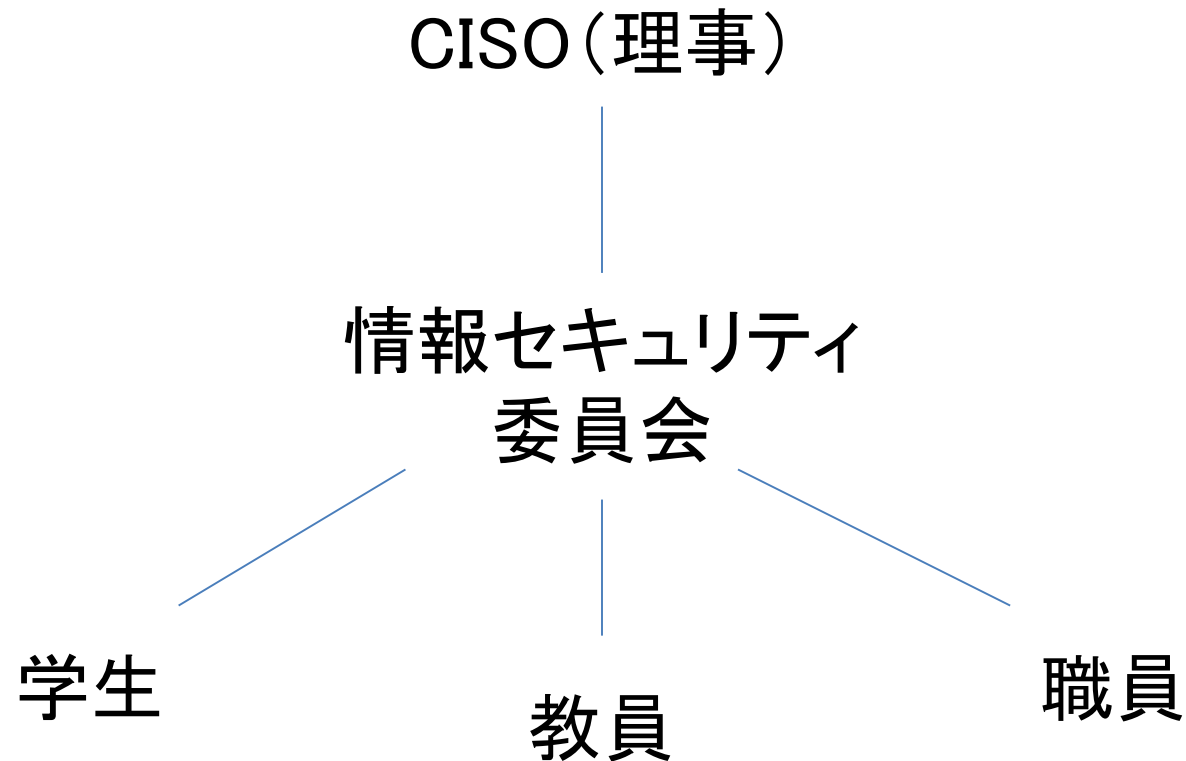
後藤滋樹

大学は攻撃され，攻撃する

- 学生の間でトロイの木馬が蔓延
- DNS amp attack, NTP amp attack
- ssh総当たり攻撃を受けるのは日常茶飯事
- その一方で...
- PlanetLab の早稲田ノードから米国のデータセンタへのポートスキャンが行われた(MITのスライス)
- 非常勤の先生のPCが踏み台に使われた

学生(と教職員)の意識を高める必要がある

早稲田大学の体制



(本発表では学生の教育を扱います)

早稲田大学における教育

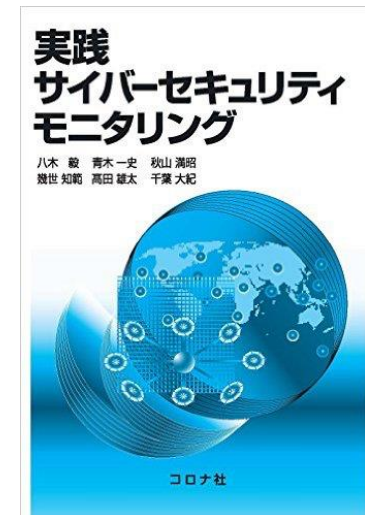
- NTT寄附講座の形で2科目を2015年度新設
- 大学院「高度サイバー攻撃対策技術」春学期
- 学部「サイバー攻撃対策技術の基礎」秋学期
- 詳しい内容を学会の研究会で紹介
八木毅, 秋山満昭, 森達哉, 針生剛男, 後藤滋樹,
「産学連携によるサイバーセキュリティ教育分野の確立」
信学技報, vol. 115, no. 81, ICSS2015-10, pp. 51-56, 2015年6月.

(参考) 既設の科目

- 学部科目「情報セキュリティ基礎」
前半は暗号と認証
後半でネットワークセキュリティを扱う
教科書: R. Lehtinen, D. Russell, G.T. Gangemi Sr.,
Computer Security Basics, Second Edition,
O'Reilly, 2006. 978-0-596-00669-3
- 大学院科目「情報セキュリティ」
暗号と認証の数学的な基礎と実例
量子暗号を含む

大学院科目 高度サイバー攻撃対策技術

- サイバー攻撃を実際に体験して対策を考える
高度な演習形式 受講できる学生数12名
- 主な内容：
攻撃の仕組み、ハニーポット、クライアントへの攻撃、サーバへの攻撃、マルウェア解析、トラフィック解析
- 授業の内容を書籍として出版
八木毅, 青木一史, 秋山満昭, 幾世知範,
高田雄太, 千葉大紀,
「実践サイバーセキュリティモニタリング」
コロナ社, 2016年 ISBN-10: 4339028533
ISBN-13: 978-4339028539



大学院科目の運営(1)

- 高度な演習を実施

受講者の人数を12人に制限

2015年度には43名が履修希望 やむなく抽選

本来は受講希望者の予備知識などをチェックして
選びたいが、履修の可否を即時に決める必要あり

- 「サイバー攻撃技術」の資料を公開できない

抽選で選外の学生のためにCourse N@vi*上に
仮想科目を設置して対象となる学生を登録した

2016年度は履修希望が12名で丁度良い

(*) Course N@viは早稲田大学の学習管理システム

大学院科目の運営(2)

- 有線ネットワーク利用可能な教室
受講者は仮想デスクトップで実験環境を利用
演習用のサーバを研究室に設置
実際には無線LANでも実施できる
- 受講者よりもTAの人数が多い
TAの大学院生は次週の予習のために時間を使う
次年度は受講経験者がTAとなる**好循環**を期待
- どこまで「お膳立て」をするか
料理教室と似たような選択
ツールのインストールは楽しみか、余分な仕事か

サイバー攻撃対策技術の基礎(1)

1. サイバー攻撃の概要とリスク

(注)一部の章の記述
を簡略化しています

2. サイバー攻撃に関わるインターネット技術

3. ポートスキャン

4. 脆弱性スキャン

5. マルウェア感染

6. 誤操作による感染

7. ソフトウェア脆弱性による感染



サイバー攻撃対策技術の基礎(2)

8. 対策を回避する高度な感染

9. 感染ソフトの遠隔操作

10. 情報漏洩、認証情報の悪用

11. DDoS攻撃

12. DNS攻撃

13. Webサイトへの攻撃

14. コンピュータネットワークセキュリティの将来

サイバー防衛人材

NTT、早大と育成

講座設置、年100人規模

NTTはサイバ女校の急増に対応し、情報セキュリティ分野の人材育成に乗り出す。2015年春から早稲田大学に講座を設けて、年間100人規模を教育する計画だ。他の企業や教育機関との連携も模索する。情報の機密流出や不正送金を狙ったサイバー攻撃に対処できる人材が不足しており、産学連携で備えを急ぐ。

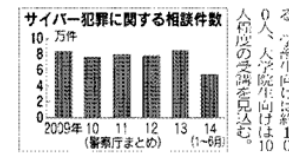
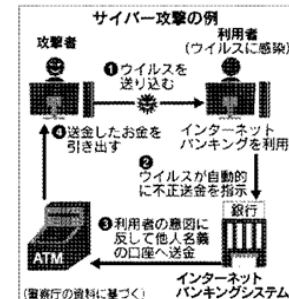
情報セキュリティ分野の第一人者のひとりである早大管理工学部の後藤滋樹教授と協力し、学部生向けと大学院生向けの2講座を新設する。学部生向けは入門編を位置づけ、攻撃の手法などを教える。大学院生向けはウイルスを使って実際に攻撃を行い、防御したりする演習も下掛ける。学部生向けは約100人、大学院生向けは10人程度を受講を見込んでいる。

NTTは情報セキュリティの研究者を随伴で大学に派遣し、実用用のサイバーやネットワーク機器も提供する予定だ。

NTTは情報セキュリティを重点分野のひとつと位置付けている。トヨタやパナソニック、日立などのNTTコムシステムを相次いで買収したほか、12年にセキュリティプラットフォーム研究所

国内では政府機関へのサイバー攻撃だけでなく、セキュリティ人材の育成も3月期に前年度5位の508万件に急増した。一し、優秀学生の採用に力、大学などで情報セキュリティのコースを修了する人材は年間約130人にとどまる。情報処理推進機構によると、同

を開設した。大学まで連携するなど、セキュリティ人材の育成を、08万件に急増した。一し、優秀学生の採用に力、大学などで情報セキュリティのコースを修了する人材は年間約130人にとどまる。情報処理推進機構によると、同



▼サイバー攻撃、メールに添付されたり、ウェブサイトに感染するなどのワイルドなIDとパスワードを盗まれたり、インターネットバンキングで他人のアカウントなどに不正送金されたりする。

昨年、ヤフーが約600万件のログイン情報が盗まれた可能性があることを発表するなど、企業が持つ個人情報を狙った攻撃が頻発している。

パソコンやスマートフォンを使わずに、解除しただけは身代金を支払えと脅すウイルスも広がっている。

上記の内容に加えて、授業では企業からの6名の招聘講師が最前線を紹介

学部科目の運営

- 教室における授業

3年生の選択科目として受講者を100名と想定して準備を進めたところ、2015度は4年生の履修者を含めて150名。2016年度は117名に落ち着く
常勤2名＋非常勤2名＋招聘講師6名
情報共有とお互いの分担の工夫
教科書が既刊であることは情報共有に有効

- 学生の高い関心

(学生の感想) 難しい内容だが、興味がある
学部1年生(学科未配属)、高校生からの質問

情報セキュリティの教育効果

- サイバー攻撃を理解するためには、情報通信技術の全般にわたる技術の理解が不可欠

ハードウェア、アセンブラ、プログラミング言語、OS、ブラウザ、電子メール、word、データベース、サーバ、TCP/IP...

- 学生が手応えを感じる機会がある
企業人が常に強いわけではない(コンテスト)
- 社会に要請されている課題であるという認識
多くの報道、絶え間ないニュース

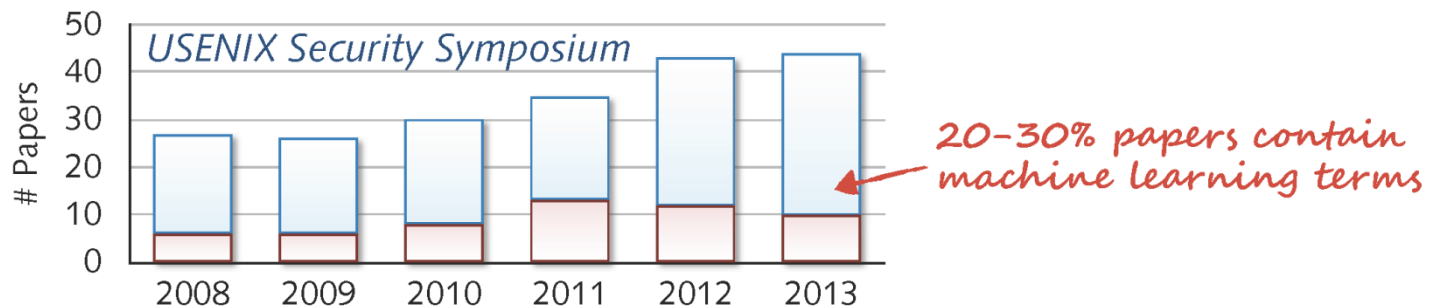
今後の課題

- 既に産学官の連携に向けての多くの努力
- 課題は情報の共有
 - 例：研究用のデータ（授業でも提示することがある）
 - black data は学会を中心とした取組みが実績を積み重ねている（情報処理学会 MWS dataset）
 - white data へのアクセスが非常に難しい（個人情報）
 - privacy-aware なデータの共有の方法
- 研究成果を、どこまで共有できるか
 - 技術の詳細を表現する方法
 - （昔：アルゴリズムを説明、今：機械学習は black box）

教育と研究は両輪

国際会議 (USENIX Security Symposium) における発表論文の20–30%は機械学習に関連する用語を含んでいる。

» ... here's a small study



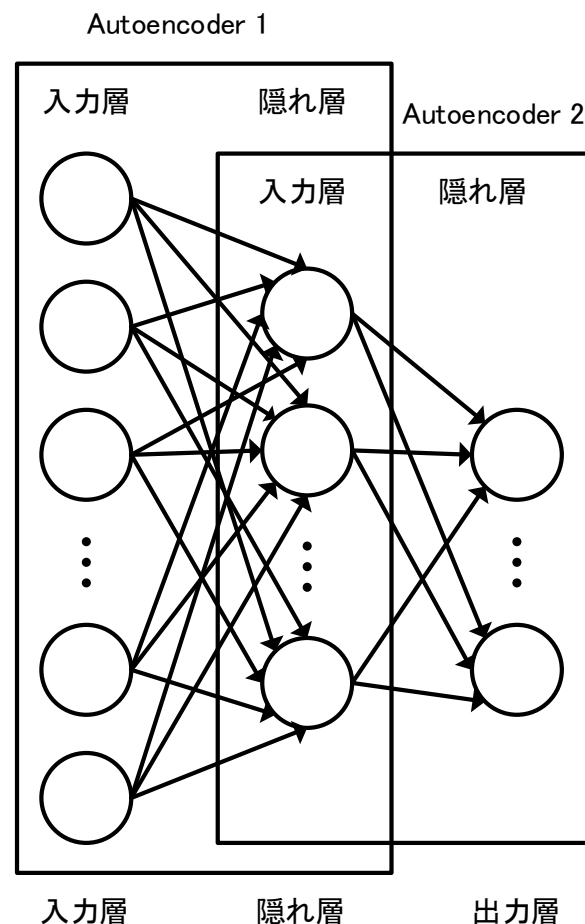
<http://user.informatik.uni-goettingen.de/~kriec/doc/2013-aisec-keynote.pdf>

例: Deep Learning の技法

Stacked Auto-encoder

Best
Student
Paper
Award

- Stacked Auto-encoder
 - 隠れ層の出力を次の Auto-encoder の入力として繋ぎ合わせる
- De-noising Stacked Auto-encoder
 - De-noising Auto-encoder を用いた Stacked Auto-encoder



国内だけでなく国際協力が不可欠

- ミサイルとサイバー攻撃は訓練が必要
近距離の方が遠距離よりも成功率が高い
ウィルスは近くのネットワークに拡散する
- 日本を攻撃してくる某国内でも被害甚大
その国でデータを収集して欲しい
人材育成にも協力(特に指導者の拡充)
- JPCERTはAPCERTをリードしている
APCERTのセッションのあるAPRICOT国際会議

拒絕服務攻擊 (DoS attack)の例



http://www.cnnic.cn/gywm/xwzx/xwzxtzgg/201308/t20130825_41322.htm

公告 2013年08月25日 10:34来源: 作者: [字号: 大 中 小] 打印

8月25日凌晨零时许, 国家域名解析节点受到拒绝服务攻击, 经我中心处置, 至2时许, 服务恢复正常, 我中心于凌晨3时许通过官方微博对用户发布了通报。凌晨4时许, 国家域名解析节点再次受到有史以来最大规模的拒绝服务攻击。部分网站解析受到影响, 导致访问缓慢或中断。

从发生攻击至发布公告之时, 我中心与国家有关部门一直在积极努力处置。截止目前, 攻击仍在持续, 国家域名解析服务已逐步恢复。

目前, 工业和信息化部已启动“域名系统安全专项应急预案”, 进一步保障国家域名的解析服务。我中心对受到影响的用户表示歉意, 对发动网络攻击影响互联网稳定的行为表示谴责。我中心将继续与国家各相关部门协同, 持续提升服务能力。

事件的最新情况, 我们将及时通过官方发布渠道向公众予以告知。

人材の育成に期待を寄せる

[1] 九州大学

サイバーセキュリティを全入学者の必修科目(西日本新聞)

CAUA FORUM 2016 岡村耕二先生の講演

<http://www.ctc-g.co.jp/~caua/event/forum2016/>

[2] 北陸先端大学 NECの寄附講座(NECの発表)

http://jpn.nec.com/press/201411/20141117_01.html

[3] 東京電機大学「高度人材養成のための社会人学び直し大学院プログラム」(文部科学省)

http://www.mext.go.jp/component/a_menu/education/detail/_icsFiles/afieldfile/2014/10/23/1352877_11.pdf

[4] 早稲田大学におけるNTTの寄附講座(日経新聞)

<http://www.nikkei.com/article/DGXLZO79116720R31C14A0TJ1000/>

注) 報道記事のリンクが古くなっている可能性があります

セキュリティ教育の課題と効果

- セキュリティへ教育の関心の高まり
産業横断サイバーセキュリティ人材育成検討会
<http://cyber-risk.or.jp/>
- セキュリティの理解のためには、情報通信の広範な知識が必修：（一部既出） マシン語、オペレーティングシステム、データベース、ネットワーク、ブラウザ、サーバ、アプリケーション(アプリ)...
- 敷居が高いが、教育的でもある
- 現在のセキュリティ人材は約26・5万人。約16万人は技術が不十分、さらに約8万人不足（読売新聞）

ウィルス感染対策に学ぶ情報共有

それを例えば周囲に明らかにしてしまうと、仲間外れにされたり、あるいはさまざまな害を受けたりということが起こりうると思います。自分の家族が患者だった場合に隠した可能性というのは十分にあります。**その病気**の家族がいてもなかなか病院に連れて行かないということはあったかもしれないです。最初60人の発症の報告がありましたけれども、そのような形で現地で広がった。

NHK クローズアップ現代, No.3539, 2014年8月25日(月)放送
“緊急事態”エボラ出血熱 ～感染拡大は止められるか～

<http://www.nhk.or.jp/gendai/articles/3539/1.html>

ゲスト 大曲貴夫さん（国立国際医療研究センター）