第4回（平成26年度第1回）CRCフォーラム（平成26年6月16日（月）開催）
「TDUにおけるサイバーセキュリティ教育と研究発表会」

TDU－MCSTRPの取り組みについて

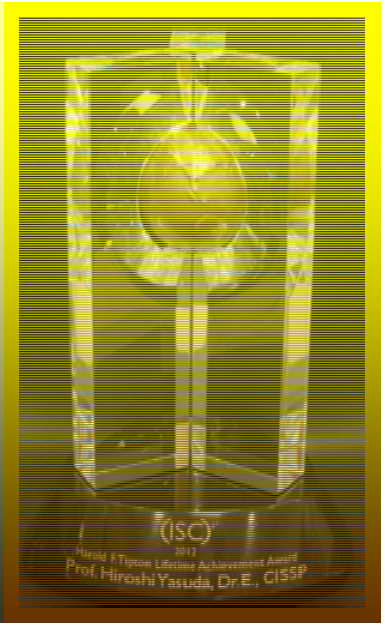
安田　浩　教授
未来科学部情報メディア学科

TDU
東京電機大学

第1回TDU－CRCフォーラム

TDUにおけるサイバーセキュリティ教育と研究　発表会

TDU－MCSTRPの取組について



平成26年　6月16日
東京電機大学　未来科学部　学部長
東京大学名誉教授
CISSP　安田　浩
yasuda@mpeg.im.dendai.ac.jp
www.mpeg.im.dendai.ac.jp

我が国の情報セキュリティ上の課題(1)

① 「サイバーテロ技術」「セキュリティ対策技術」に精通した人材が不足しており、問題が生じた際においても的確な対応を実施できる人材は希少であること。
→セキュリティ高度専門技術者の不足

② ネットに接続される端末(PC、サーバ)自体の汚染、ネット空間そのものの汚染に耐えうる根本的な対応技術が存在しないこと。
→国産セキュリティ技術の不足

③ 既存のセキュリティアプライアンスにより、「侵入は仕方ない」「出口で防ぐ」という対策が一般化され、「サイバーテロ攻撃」による破壊工作への耐性があまりにも脆弱であること。
→セキュリティ技術高度運用者の不足

我が国の情報セキュリティ上の課題(2)

④ セキュリティ法整備・対策基準・各種ガイドライン等が古く、それを順守し対策を講じただけでは、日進月歩で進化する「サイバーテロ技術」に追いつくことはもちろん、防御することすら不可能な状況にあること。
→セキュリティ政策高度運用者の不足

⑤ 社会活動の中でセキュリティの必要性・重要性を自覚した者に対する効果的な教育システムが存在しないこと。
→セキュリティ教育の生涯教育化の遅れ

⑥ セキュリティ教育を受けても必ずしも有利な職が得られない等セキュリティキャリヤパスが充実していないこと。
→セキュリティ学位が存在せず

セキュリティ教育・研究強化の目的

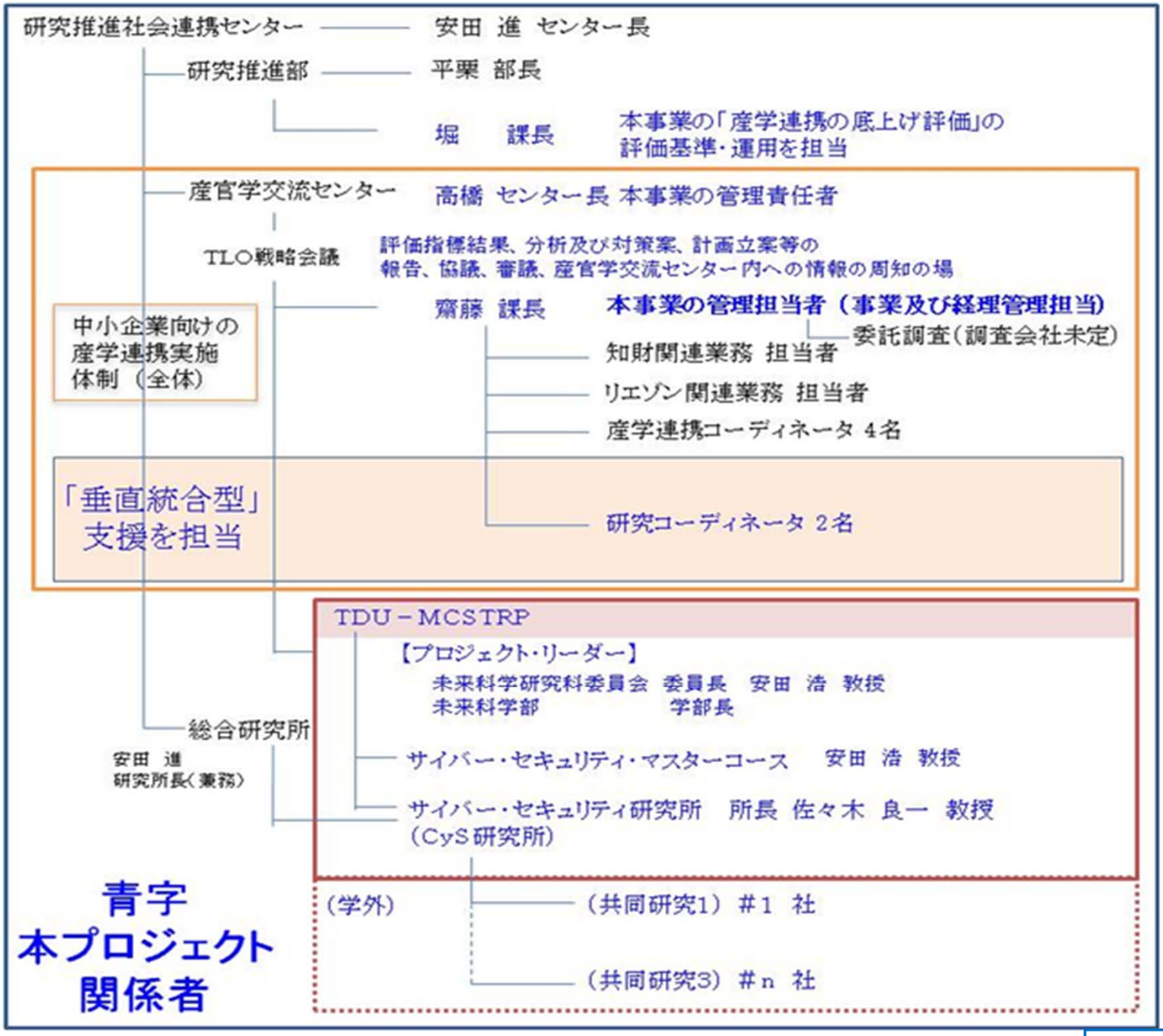
ア） サイバー・セキュリティ高度専門技術者の育成

イ） 国産「複合領域サイバー・セキュリティ技術」の研究・開発

ウ） サイバー・セキュリティ政策・技術高度運用者の育成

エ） サイバー・セキュリティ社会人教育制度の設置と新学位の創設

TDU－MCSTRPの設立



GCSMコースの内容

① 心理学(犯罪・行動)・精神分析・数学・統計学等

② 倫理学・法学・経済学等

③ セキュリティ核技術(CISSP・CBKを中心:別紙1参照)

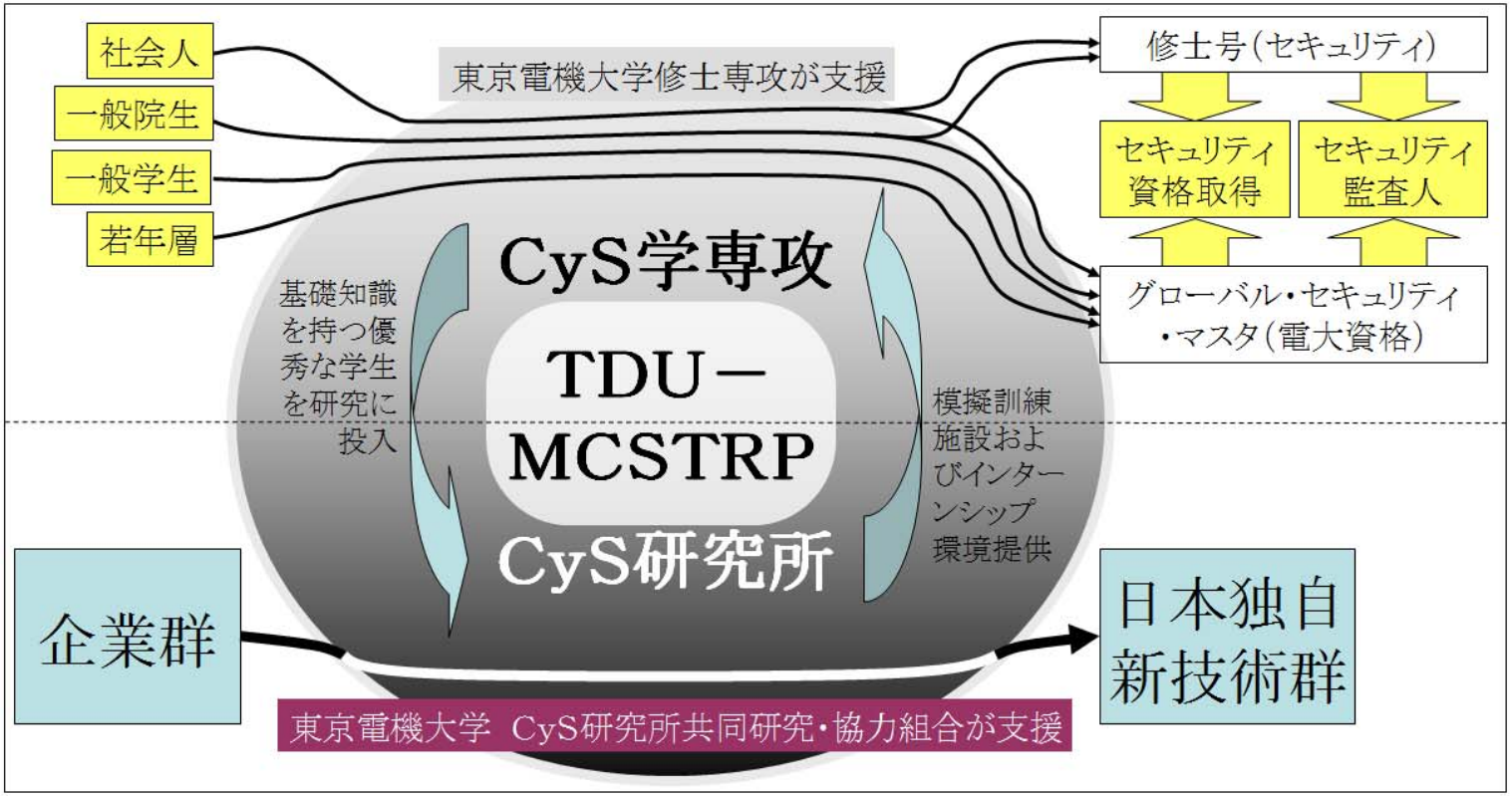
④ システム設計開発・事業継続計画・サービス開発等

⑤ ガバナンス(統制力・交渉力・コミュニケーション力等)

⑥ 脆弱性監視・検査技術等の実習(サイバーセキュリティ研究所)・インターンシップ(共同研究企業・本専攻支援企業)

TDU-MCSTRPの概要

TDU－MCSTRP：Tokyo Denki University-Multidisciplinary Cyber Security Technology Research Project
東京電機大学　複合領域サイバ・セキュリティ技術研究開発プロジェクト



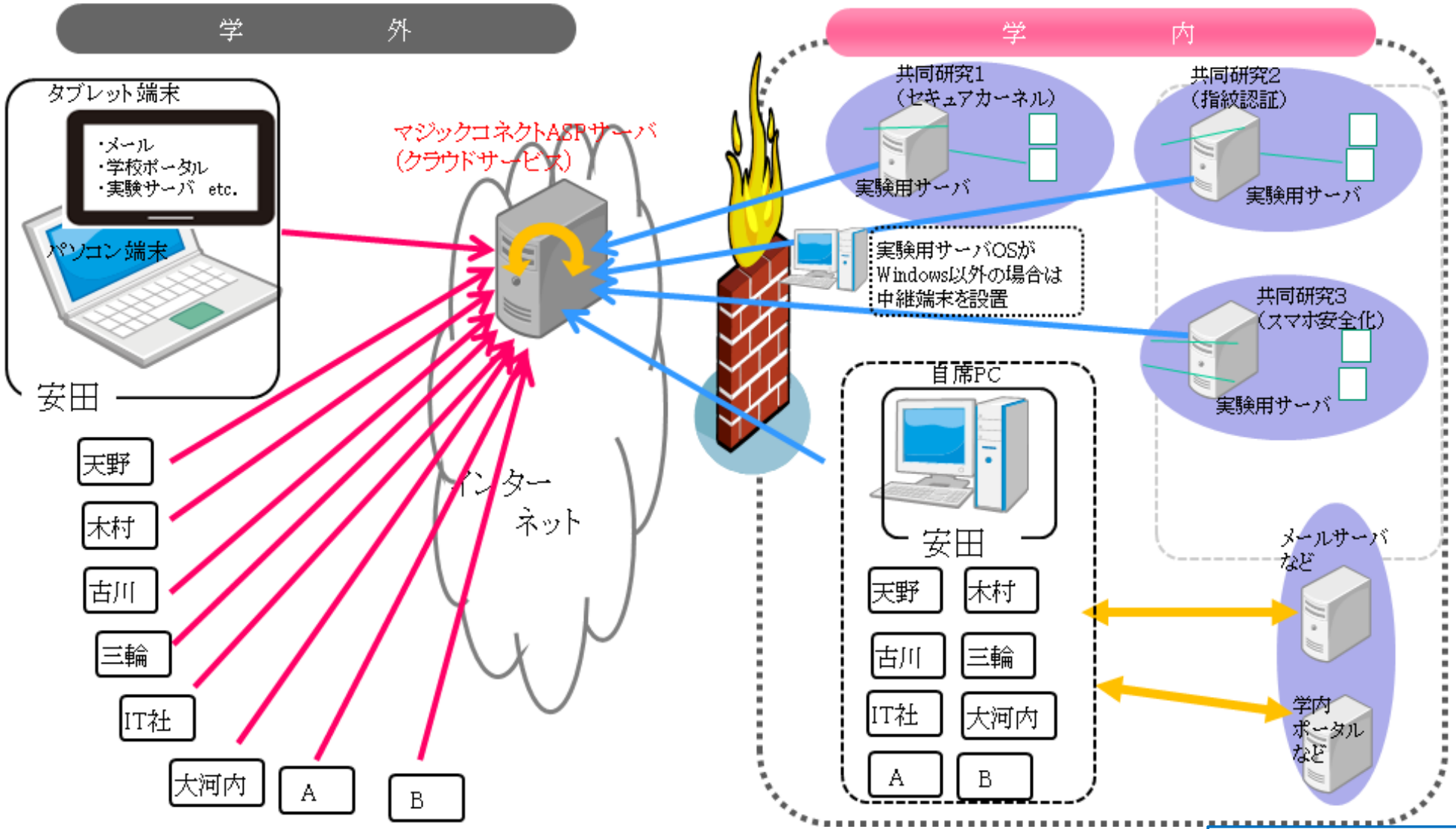
TDU－MCSTRP　の　目的

目的1　CyS研究所での実習により若年層も含み実践的高度セキュリティ技術者育成を行う
目的2　英語講義を100％化しグローバル高度セキュリティ技術者育成を行う
目的3　総合的セキュリティ教育を行いCEO，COO、CFO、弁護士、弁理士、税理士等のCS意識向上を図る
目的4　修士コース・社会人等の優秀な人材をCyS研究所に投入し最先端CyS国産技術を実用化する
目的5　共同研究・インターンシップの実施により、緊密かつ幅広い産学連携活動を行う

TDU-MCSRRのNW構成

もう一つの実験

Office Free かつ 作業エビデンスが確実に収集可能なシステムを構築



今後の進め方(1) 骨子

1年目(平成26年)

○ 端末/サーバ安全化技術を電大サーバに実装し、攻撃者を募って耐性を確認する共同実験を行う。

○ 端末/サーバ安全化技術によるセキュアID空間の構想を完成する

2年目(平成27年)

○ セキュア空間を構築し、セキュアIDが提供できることを実証する

○ セキュア空間の構築・ライセンス提供体制等に構想を完成する

3年目(平成28年)

○ 使用頻度の高い全OSならびにそのバージョン変化に対応できるよう端末/サーバ安全化技術の研究開発を進め、完成度を高める

4年目(平成29年)

○ セキュア空間をすべての応用分野で展開できるよう開発を進め、体制を整える

今後の進め方(2) 本年度

① 電大サーバに端末/サーバ安全化技術を実装し、攻撃標的となる環境を作る

仮想インターネットの構築を必要とする。
またログ採取のためには、技術のある会社との連携を模索する
以上の内容を6月末までに完成、日本並びに米国で発表する

② 7月―10月で攻撃者をつのり、攻撃させることにより耐性の検証を行う

攻撃チームの剪定・依頼を行う、自発的応募歓迎

③ セキュアID空間の構想を具体化する

10月末設計仕様完成
端末/サーバ安全化技術の啓発をはかり核組織を作る
→経営層へのサイバー・セキュリティ・トップ・セミナー実施
→複合領域サイバー・セキュリティ実践組織の構築

④ シンポジウム、啓発活動、外部組織との連携活動を強化する

2020年東京オリンピック
はICTオリンピックです
皆の力で守り抜こう