KYUSHU UNIVERSITY

Kyushu University 2011
100th Anniversary

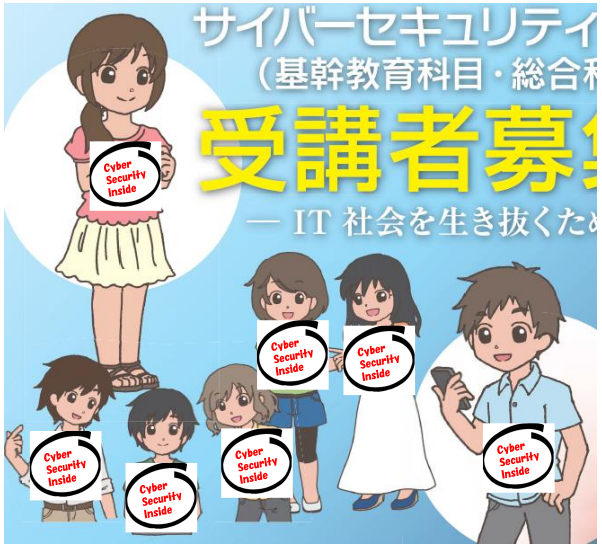
Introduction of Cyber Security Center

Koji OKAMURA
Director, Cyber Security Center, Kyushu University

Mission

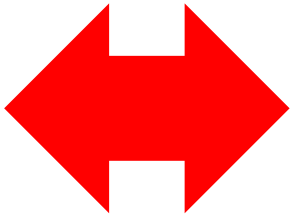
- Improvement of Cyber Security Level of Kyushu University
  - Primary Course
    - Security aware student
  - Advanced Course
    - Security aware researcher
  - Specialist Course
- Advanced Practical Research
  - Advanced Cryptography
  - Advanced Defense against new Cyber Attacks
- Exploring New area of Cyber Security
  - Social Security
  - Security and Economy
  - Security and Law

- Background
  - World Wide Cyber Security Attack Threats
    - Economy
    - Social Infrastructures
  - Nation Strategies
- Chance
  - Collaborations with UMBC



Departments and Cooperation

- **Education** for Cyber Security
- Advanced **Technologies** for Cyber Security
- **Social** Cyber Security
- **International** Collaboration
- Company Cooperation (in Future)



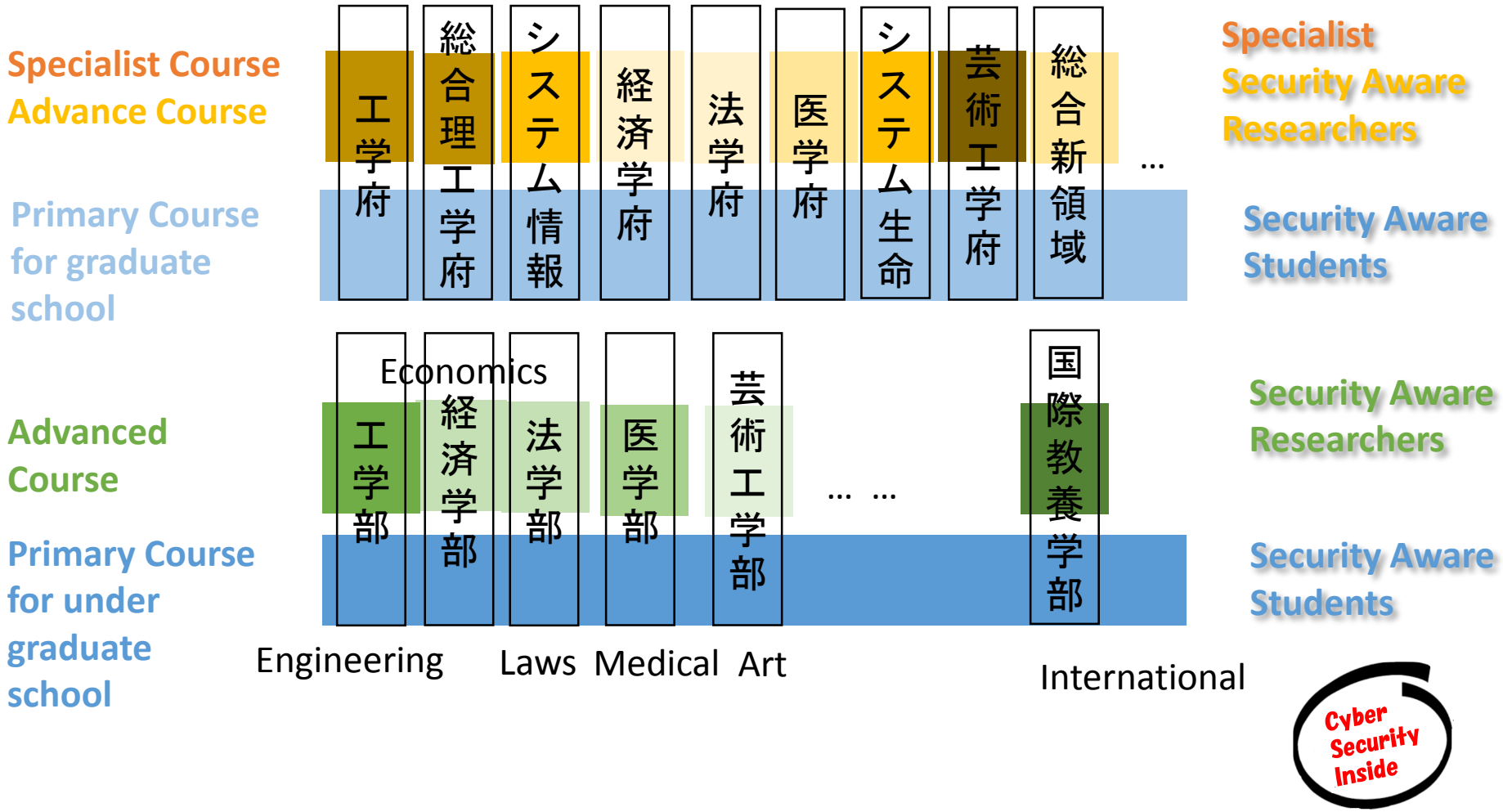
- Faculty of Information Science and Electrical Engineering(ISEE), Law, Economics and Arts and Science
- Institute Mathematics for Industry(IM)
- Innovation Center for Educational Resource
- Medical Information Center(MIC)
- Research Institute for Information Technology (RI2T)

Activities and Expectation

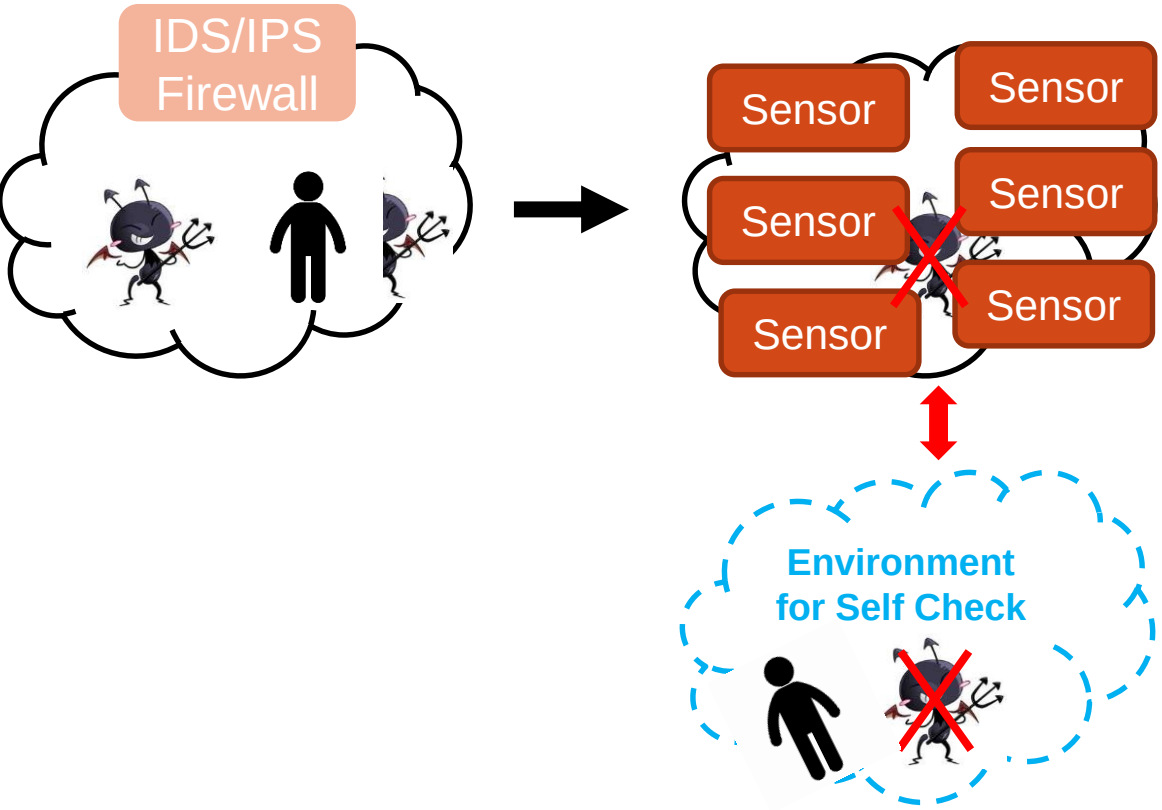
- **International** Level and Quality Cyber Security Education
- **Practical** Research, Education and Operation
- **Active** Defense Strategy
- Cyber Security **Social Science**

- Caring out Nation Strategies as University
- International Education and Research
- Contribution to real world and life
- Keeping Continuous Activity

Cyber Security Educations

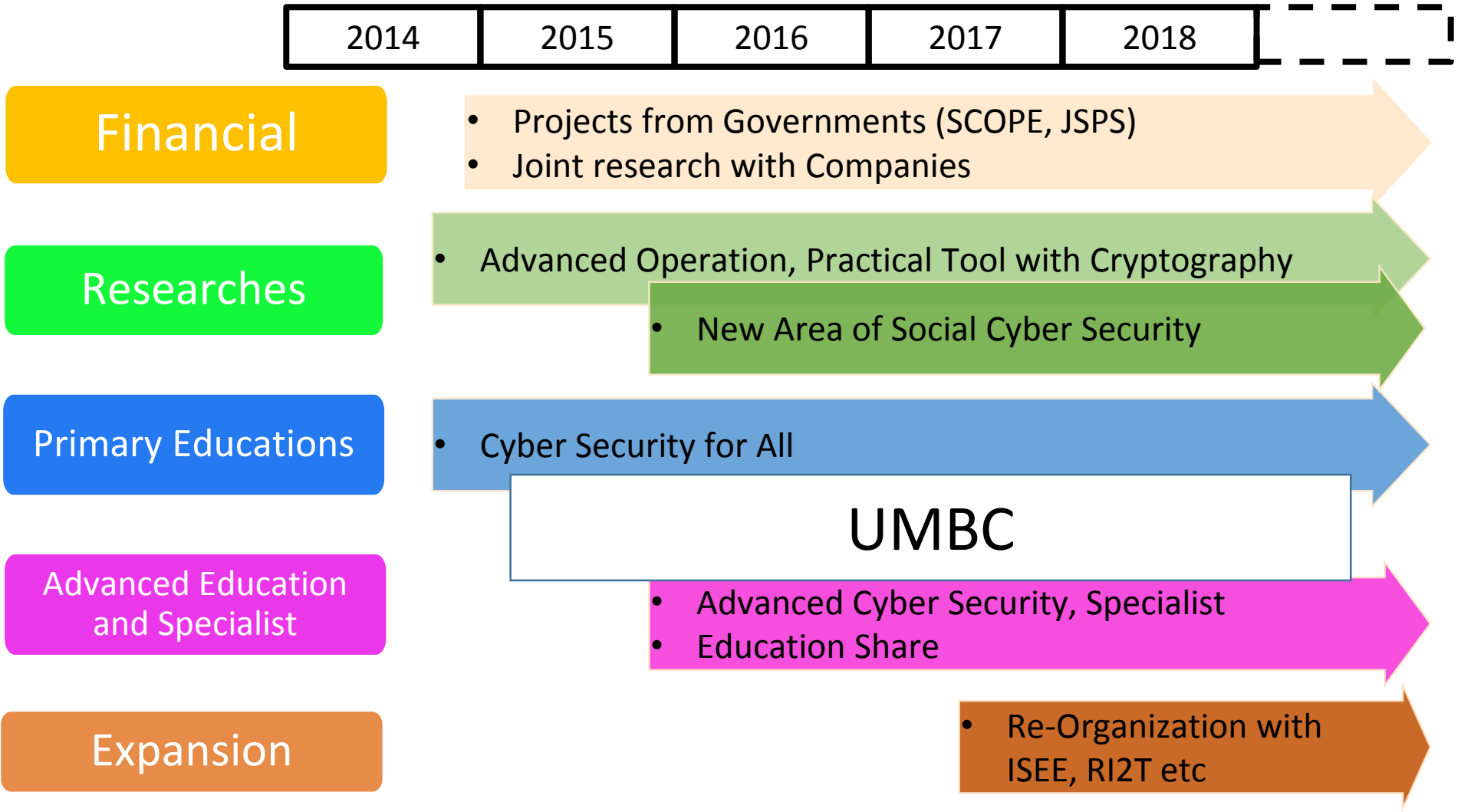


APT (Advanced Persistent Threat), Zero Day Attack

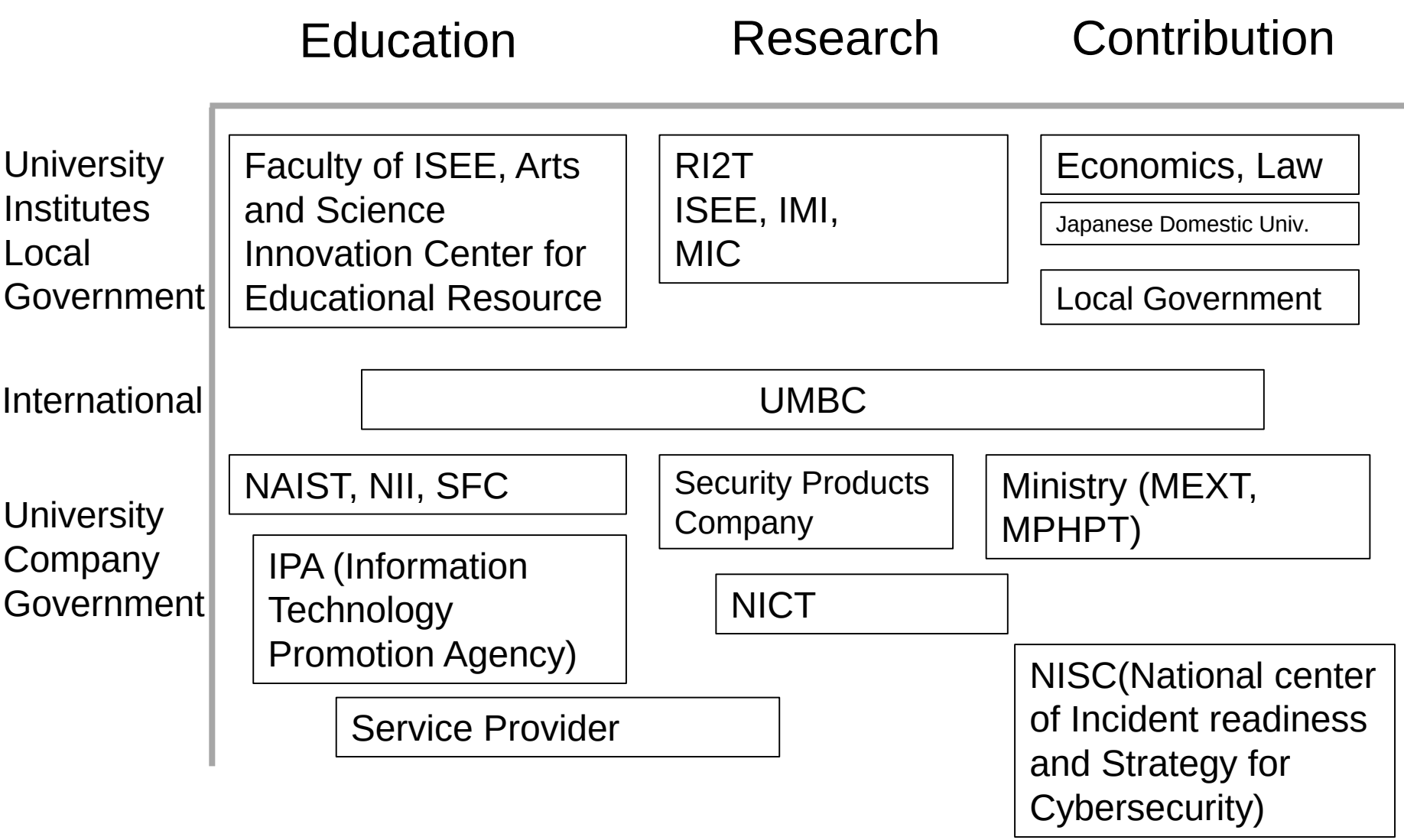


- Collaboration/Cooperation with Companies, Institutes and University in Japan and World
- Research and Operation in real networks
- Active Strategy

Roadmap


2014
2015
2016
2017
2018
Financial
• Projects from Governments (SCOPE, JSPS)
• Joint research with Companies
Researches
• Advanced Operation, Practical Tool with Cryptography
• New Area of Social Cyber Security
Primary Educations
• Cyber Security for All
UMBC
Advanced Education and Specialist
• Advanced Cyber Security, Specialist
• Education Share
Expansion
• Re-Organization with ISEE, RI2T etc

Partnership



参考資料

背景：我が国のサイバーセキュリティを取り巻く状況

- 急激に増加するサイバー犯罪
  - サイバー犯罪の損失額は全世界で年間59兆円
  - 日本の政府機関を標的にしたH25年度のサイバー攻撃は約508万件（→前年度に比べ5倍に急増）
  - 手口も巧妙化→サイバー攻撃の脅威は急速に拡大
  - サイバーセキュリティの被害者の6割強が18歳から31歳
    - 被害者が間接的な加害者になるリスク

- 状況の変化は極めて急速、問題は拡散し、グローバル化
  - 「国家安全保障」や「危機管理」上の最重要課題
  - 重要インフラの防護に最善の措置の導入が不可欠
  - 情報の自由な流通を確保し、常に深刻化するリスクに対し新たな対応の強化が必要

背景：我が国のサイバーセキュリティへの取り組み

- 我が国：世界最先端のIT国家の構築に取り組んでいる
  →それにふさわしい安全なサイバー空間の実現が必要
- 政府：従来の情報セキュリティ確保の取り組みはもとより、広くサイバー空間に係る取り組みを推進する必要性と体制を明確化するため、サイバーセキュリティ戦略を策定
  - 政府は2020年東京五輪の開催を見据え、政策会議を法制化し、平成27年度にも「サイバーセキュリティ政策会議」に格上げ
  - H27年度総務省重点施策に「サイバーセキュリティの強化」として15.2億円計上するなど、関連する施策を強化

内閣官房情報セキュリティセンター・情報セキュリティ政策会議・H27年度科学技術関係予算概算要求より

大学として最先端のサイバーセキュリティを実現するための行動必要

サイバーセキュリティセンターの構成(案)

サイバーセキュリティセンター

サイバーセキュリティ教育のデザイン
- 基幹教育
- 国際教養学部(仮称)教育
- 学部教育
- 大学院教育
- 専門教育

サイバーセキュリティ研究
- 高度基礎研究
- 運用研究

グローバル教育・研究
- 北米連携(メリーランド大学)
- ヨーロッパ連携
- アジア連携

<u>サイバーセキュリティ教育部門</u>
- 専任教授(基盤セより配置)
- 兼任教授(基幹教育院, 教材開発セ)
- 兼任准教授(システム情報)
- 兼任助教(MIC)

<u>高度セキュリティ技術研究部門</u>
- 兼任教授(システム情報, IMI)
- 特任准教授(企業)

<u>社会情報研究部門</u>
- 兼任教授(法学研究院)
- 兼任教授(経済学研究院)
- 兼任助教(基盤セ)

<u>海外連携部門</u>
- 特任教授(メリーランド大学)
- 特任准教授(メリーランド大学)

<u>企業共同研究</u>
- 学生向け実用講義
- 企業人向け高度セミナー

サイバーセキュリティ連携
- 組織内連携
  - 情報統括本部
  - 施設部、情報システム部
- 大学連携
- 政府連携, NISC
- 研究所、企業連携
  - NICT、JPCert、IPA
  - セキュリティ関連企業(富士通、NEC、日立、など)
- 国際連携

事例研究・サイバーセキュリティ対策運用研究
- 組織内CSIRT (Computer Security Incident Response Team)

共同研究部門への展開

サイバーセキュリティセンターの将来構想

サイバーセキュリティ教育プログラムの研究開発
- 基幹教育
- 国際教養学部教育
- 学部教育
- 大学院教育
- 専門教育

サイバーセキュリティ研究
- 安全・安心のための研究
- 高度防御研究

社会国際連携研究
- メリーランド大学
- 情報倫理・法律
- セキュリティインシデントによる負の経済影響

目標

世界標準の大学・大学院のサイバーセキュリティ総合教育プログラムの開発

セキュリティ対策技術の**実用化**：教育、研究、事務活動の向上に貢献

戦略的セキュリティ対策：受け身ではない、能動的な対セキュリティ技術

サイバーセキュリティ**社会科学**

効果

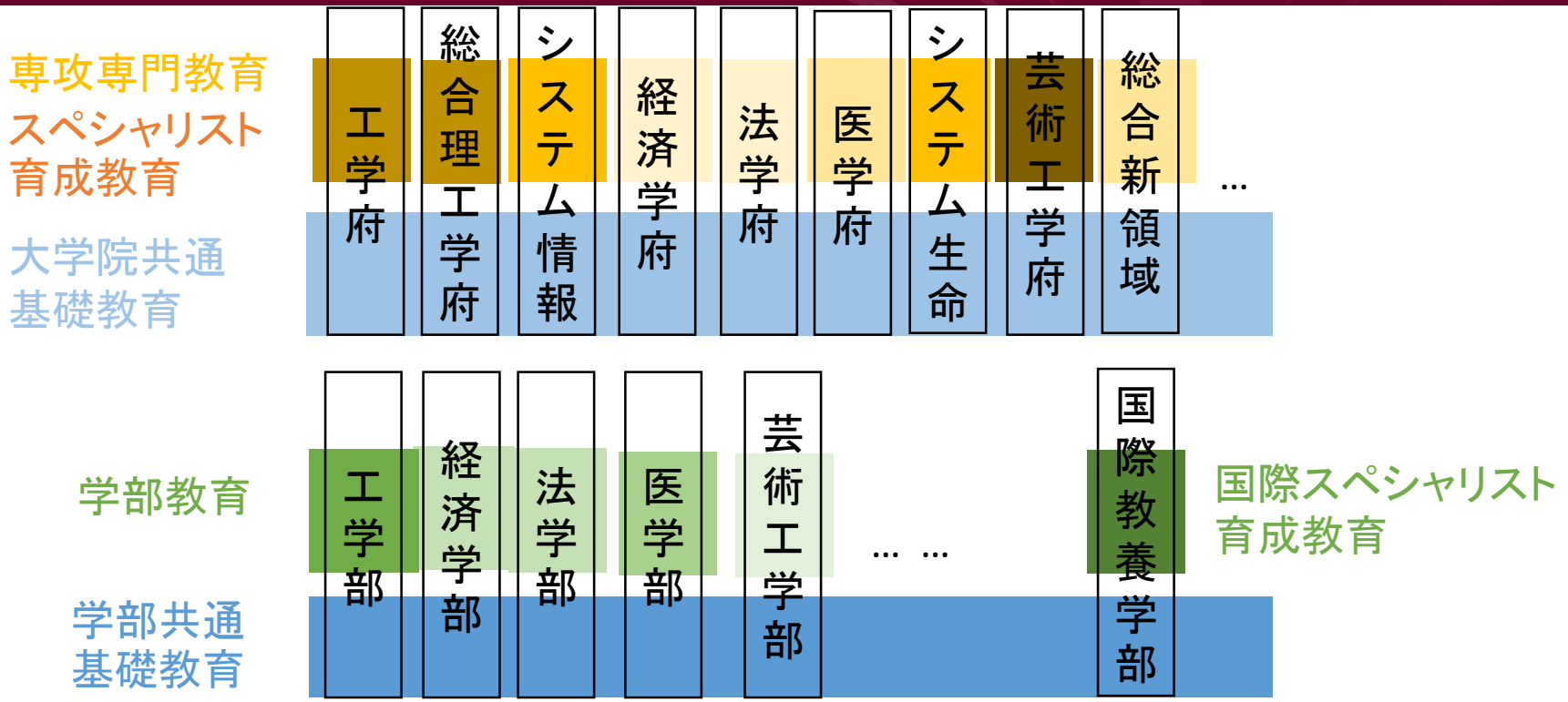
大学として**国の責任を果たす**
・サイバーセキュリティ基本法順守
・リテラシの向上
・人材育成
・高度な技術開発

グローバル化
・UMBC
・世界展開

社会貢献
・実用的なセキュリティ技術

将来性
・**永続的**・陳腐化しない

サイバーセキュリティ総合教育



- シラバス
- 教育レベルの選択
- 教材

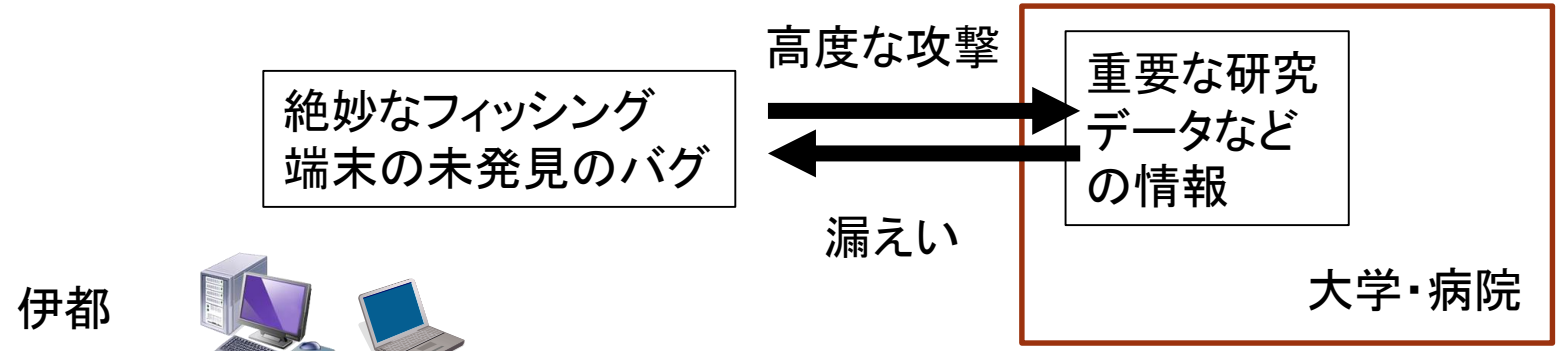
サイバーセキュリティに関する専門知識
教育の質の保証（世界標準）
学部・専攻別に必要になる知識の分類
スペシャリスト育成に必要な要件

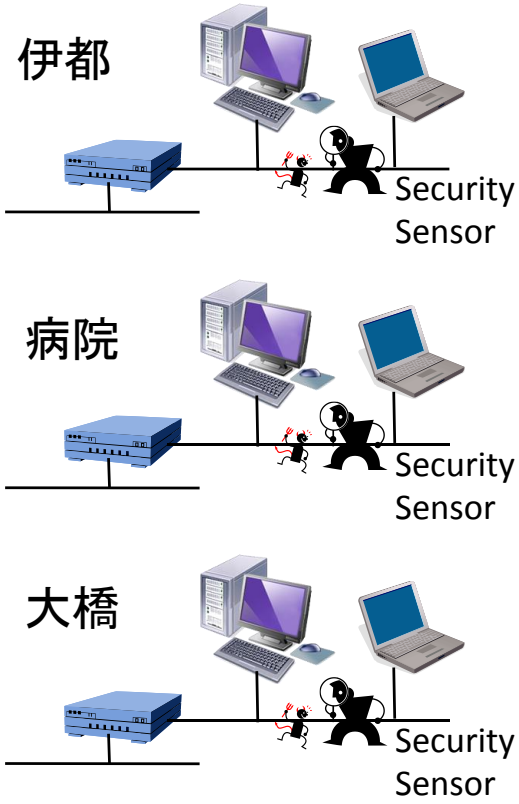
情報レイヤ　多角的な視野が必要
横断的レイヤ
政治レイヤ
グローバルレイヤ

UMBC 連携

世界標準となる学部～大学院
サイバーセキュリティ総合教育プログラムの研究開発

標的型攻撃への対応





- 標的型攻撃は、数年前からアメリカでの被害が始まり、現在では日本の主要な企業の被害も出始めている。
- 数年、数か月で、日本国内の大学にも被害が出ることは自明
- アンチウイルスなどと違い、対処できるシステムは存在しない
- 全学・全支線にセキュリティセンサーを設置
- リアルタイム処理
- 外部との連携、情報収集が必須
  - 企業、国内外研究機関との共同研究
  - 基礎研究　＋　運用能力 が必要
  - 戦略的セキュリティ対策研究

スケジュール案

2014年度	2015年度	2016年度	2017年度	2018年度

教育研究開発拠点の整備，競争的資金，概算要求

- プロジェクト申請（大型科研費，CREST，SCOPE他）
- 企業等との共同研究検討
  →複数企業参画による共同研究部門（COOPプログラム）

先端／連携研究の推進

- サイバービッグデータから未知の脅威を発見する技術の開発
- サイバーセキュリティにまつわる法制度や社会現象の研究
- プライバシー保護，サイバー犯罪抑止技術の開発

基礎教育プログラムの開発・基幹教育の実施

- 基礎教育用プログラムの開発
  - 基幹教育での実施
  - 全ての学生が受講できるようカリキュラムの調整
    Cyber Security for All

先端教育プログラムの開発・プロフェッショナル育成

- 先端教育プログラムの開発
  - 専門的な知識を身につける教育プログラムの開発
    - 学部、大学院への提供、一部で実施
  - UMBCとの連携に基づくEducation Share
  - 国際教養学部（仮称）での専門教育の設計と実施
- 先端プログラムによるプロフェッショナル育成
  - 企業と共同実施，社会への成果フィードバック

センター組織の拡充

- 情報基盤研究開発センター，システム情報科学研究院，その他サイバーセキュリティに関連する部局等で全学的に，拡充計画を検討し，実施

協力体制

	サイバーセキュリティに関する教育開発	安全・安心なインフラ実現に関するする	社会・国際連携、貢献
九州大学 教育機関 自治体	基幹教育院 システム情報 教材開発センター	情報基盤研究開発センター システム情報、IMI 病院	経済学、法学 日本国の他大学 自治体
国際連携	メリーランド大学 UMBC		
産学官連携	奈良先端科学技術大学院大学 国立情報学研究所 慶応大学SFC	セキュリティ製品開発企業	文科省 総務省
	セキュリティ系研究機関(NICT)		
	情報処理推進機構(IPA)		NISC(内閣官房情報セキュリティセンター)
	サービスプロバイダ系企業		