IT安全の研究戦略

RISEC

- 日米のサイバーセキュリティ戦略
- AIST情報系でのRISECの役割と研究方針
- 生命型セキュリティ戦略

2012年9月

研究部門長　松井俊浩

米国のセキュリティ政策

- FISMA法 2001
  - 連邦政府のセキュリティ、NISTの役割
- 国土安全保障省 DHS 2002 → DOE labs.
- Obama's Cyberspace Policy Review
  - サイバーセキュリティは、大統領のマネジメントの優先事項
    - サイバーセキュリティ調整官の指名、横断的体制
    - 国家的啓発・教育キャンペーン、国際連携
    - プライバシー、人権に配慮したID管理
  - デジタルインフラの信頼性、障害からの回復のためのgame changingな技術の研究開発

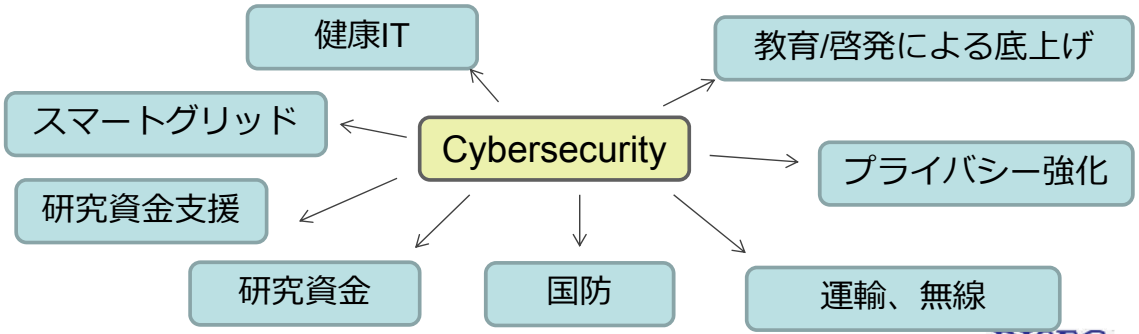
米国サイバーセキュリティ研究開発戦略の概要

- 研究は単にサイバーセキュリティの問題に対処するのではなく、問題の根本原因を理解することに注力する。
- サイバーセキュリティは多面的な問題であり、戦略は幅広い分野の様々な専門知識とリソースを取り入れる。
- 技術や脅威の環境の変化に関わらずセキュアな環境を維持するため、サイバーセキュリティの原則を堅持する。

Cybersecurity Game-Changing R & D Recommendations

NITRD Cyber Security and Information Assurance Interagency Working Group

- 変化の誘発 → 研究開発
- セキュリティサイエンス(SoS)
  - 異分野の知識融合、普遍的法則の発見、科学的厳密性
- 研究インパクトの学際的・商業的波及



変化の誘発 -研究テーマ

- Designed-In Security
  - セキュアなソフトウェアエンジニアリングシステム
- Tailored Trustworthy Spaces
  - ユーザの状況に応じた適切なセキュリティ要件が実現される高信頼環境
- Moving Target
  - 動的に変化することで攻撃の困難さとコストを上昇させ攻撃にさらされても悪影響を受けにくいシステム
- Cyber Economic Incentives
  - サイバーセキュリティへの適切な投資判断を可能にする、科学的な指標等の提供

日本のサイバーセキュリティ戦略

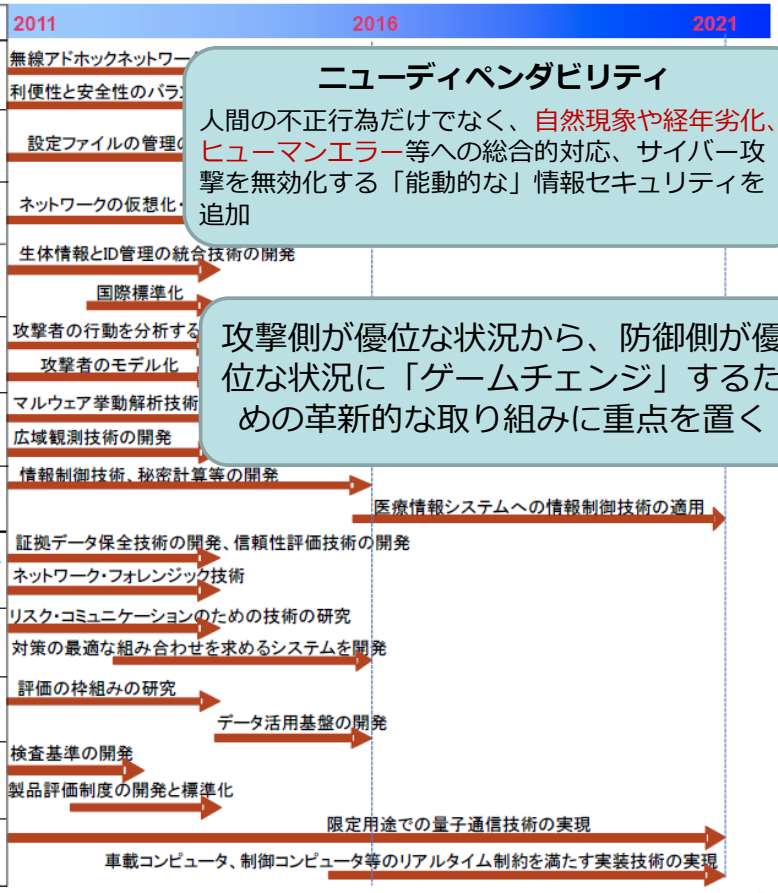
- インターネット元年 1995
- 内閣官房情報セキュリティセンター 2005
- 産総研情報セキュリティ研究センター 2005
- IT戦略本部 2005
- 第1次情報セキュリティ基本計画 2006-2008
  - ITにおいて、セキュリティは重要事項
  - 対象領域
    - 政府、自治体　→　政府機関統一基準
    - 重要インフラ
      - 行政、情報通信、鉄道、航空、電気、ガス、水道、金融、医療、物流
    - 企業, 個人　→国民を守る情報セキュリティ戦略－2010.5
  - 年度計画　- セキュア・ジャパン20XX

第２次情報セキュリティ基本計画　2009.2

- 事前の完全な無謬性は期待できない
- 事故前提社会
  - •被害を限定し、事後の回復も重視(resilience)
  - •コストやサービスとのバランス
  - •事故・障害情報の共有
- 設計段階でのセキュリティの作り込み

重要分野の研究開発ロードマップ（イメージ）

	重要分野	投資型
ニューディペンダビリティの確保	実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術	イノベーション型
	システムのセキュリティ設定を上位から下位まで自動保証する技術	長期基盤型
	障害に対して自動回復可能なネットワーク構築技術	長期基盤型
	生体情報をコンピュータで管理するためのID管理と生体情報を統合するシステム設計技術	緊急対応型
ゼロデイ・ディフェンス	攻撃者の行動分析等による予防基盤技術	イノベーション型
	大規模ネットワークにおける広域観測技術とマルウェアの挙動分析技術の統合	緊急対応型
柔軟管理の実現	個人情報等の利活用を促進する自己情報の統制技術	長期基盤型
	フォレンジック等を支援するためのデータ管理・追跡技術	緊急対応型
	ITリスクに関する理論から実務までの体系化	イノベーション型
研究促進基盤の確立	情報セキュリティ研究の理論の体系化	長期基盤型
	セキュリティ部品が正しく実装されていることを保証する製品評価認証技術	イノベーション型
	情報理論的安全性を備えた暗号技術	長期基盤型



ニューディペンダビリティ

人間の不正行為だけでなく、自然現象や経年劣化、ヒューマンエラー等への総合的対応、サイバー攻撃を無効化する「能動的な」情報セキュリティを追加

攻撃側が優位な状況から、防御側が優位な状況に「ゲームチェンジ」するための革新的な取り組みに重点を置く

取り組むべき課題

安全への脅威

自然災害
環境破壊
故障
労働災害
過失
ヒューマンファクタ
設計不備
感染症
軍事行動
悪意-犯罪
テロ

守るべき資産

機械
IT機器
産業インフラ
情報資産
サービス
個人情報
健康
経済活動
自由
領土

技術開発だけでなく、制度やインセンティブ、人材育成も重要

産総研の情報系技術マップ

セキュアシステム研究部門

システム安全
情報セキュリティ、コンテンツ配信、情報漏洩
信頼性、システム検証
ヒューマンファクタ、機能安全

シミュレーション
実世界の仮想表現

ロボット安全
事故予防

量子暗号

知能システム研究部門

人間情報
視聴覚メディア・認識技術
人間モデル、認知モデル
サービス工学
実世界情報、リアルタイムシステム
ロボット、生活支援

認知心理

フロンティア
量子計算
脳型コンピュータ
社会のIT活用
創発・集合知

メディア処理

情報技術研究部門

高性能計算(HPC)
大規模並列・分散計算
大規模データ (big data)
計算科学
グリーンIT

インターネット、情報共有
ネットワーク

クラウド
セキュリティ

バイオCAD
メノテクT-CAD
GEO-Grid
スマートグリッド

著作権
オープンソース
国際標準

情報セキュリティ問題

- 暗号系の危胎化、ハッシュ関数の衝突
- 情報漏洩、著作権侵害
- 個人認証、バイオメトリクス
- 異常・侵入検知、ログ解析
- ICチップ、サイドチャネル攻撃
- ウィルス、マルウェア、スパイウェア
- フィッシング、SPAM、ボット
- 標的型攻撃
- システムリスクの評価・算定法
- フォレンジックや事故分析技術
- プライバシ保護、国民ID

サイエンスとしてのセキュリティ
包括的・根本的な解決
多面的な研究の融合

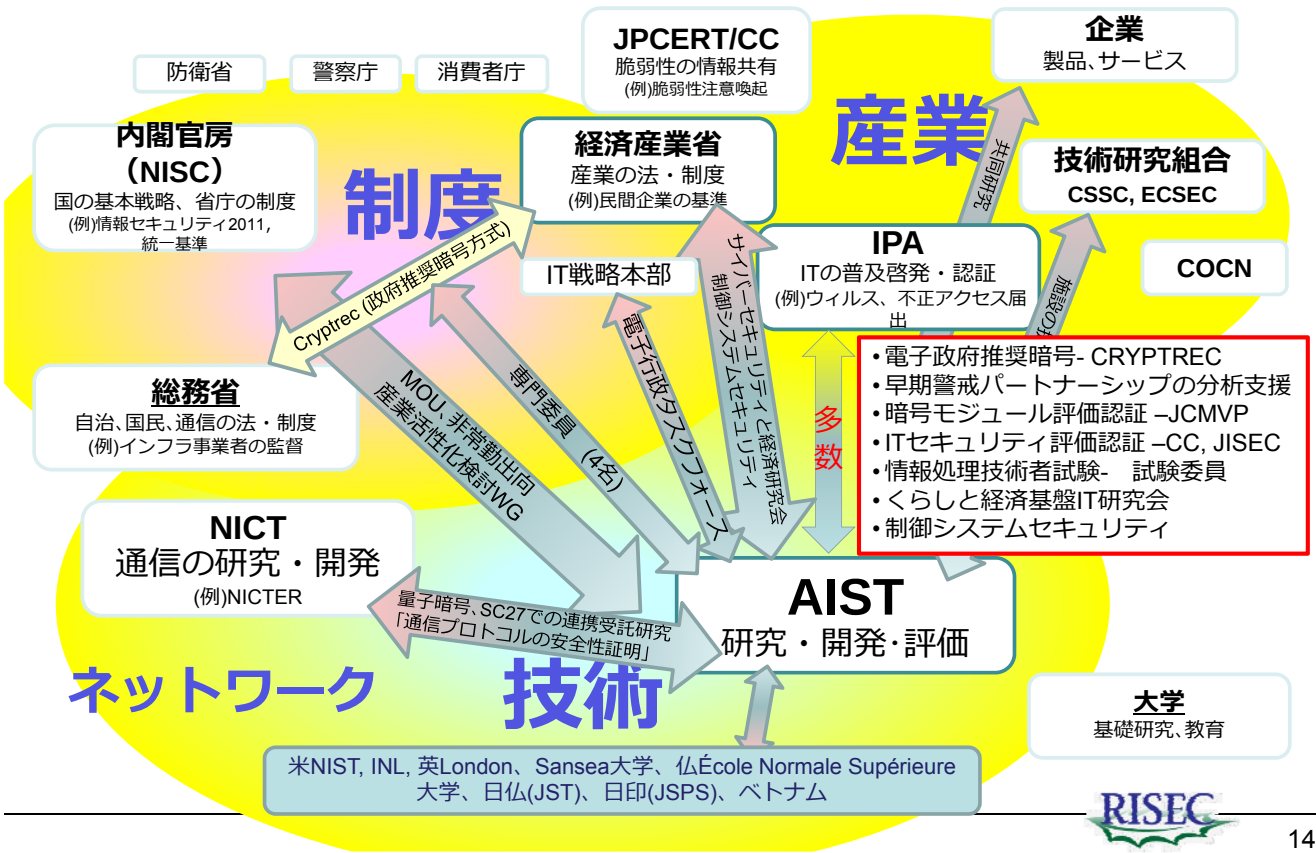
- 先端セキュリティ技術開発
  - 基盤技術
    - 高機能暗号、暗号評価、認証鍵管理、マルウェア検出
  - 具体的対策
    - コンテンツ配信、DBの秘密検索、ロボットのシステム安全
- 安全性評価
  - セキュリティ、ICチップ、信頼性の国際標準
  - 制度やガイドラインへの技術支援
- 運用
  - ヒューマンファクタ
- 設計
  - 仕様からの実装生成、テスト生成

RISECの研究テーマ概要

RISEC

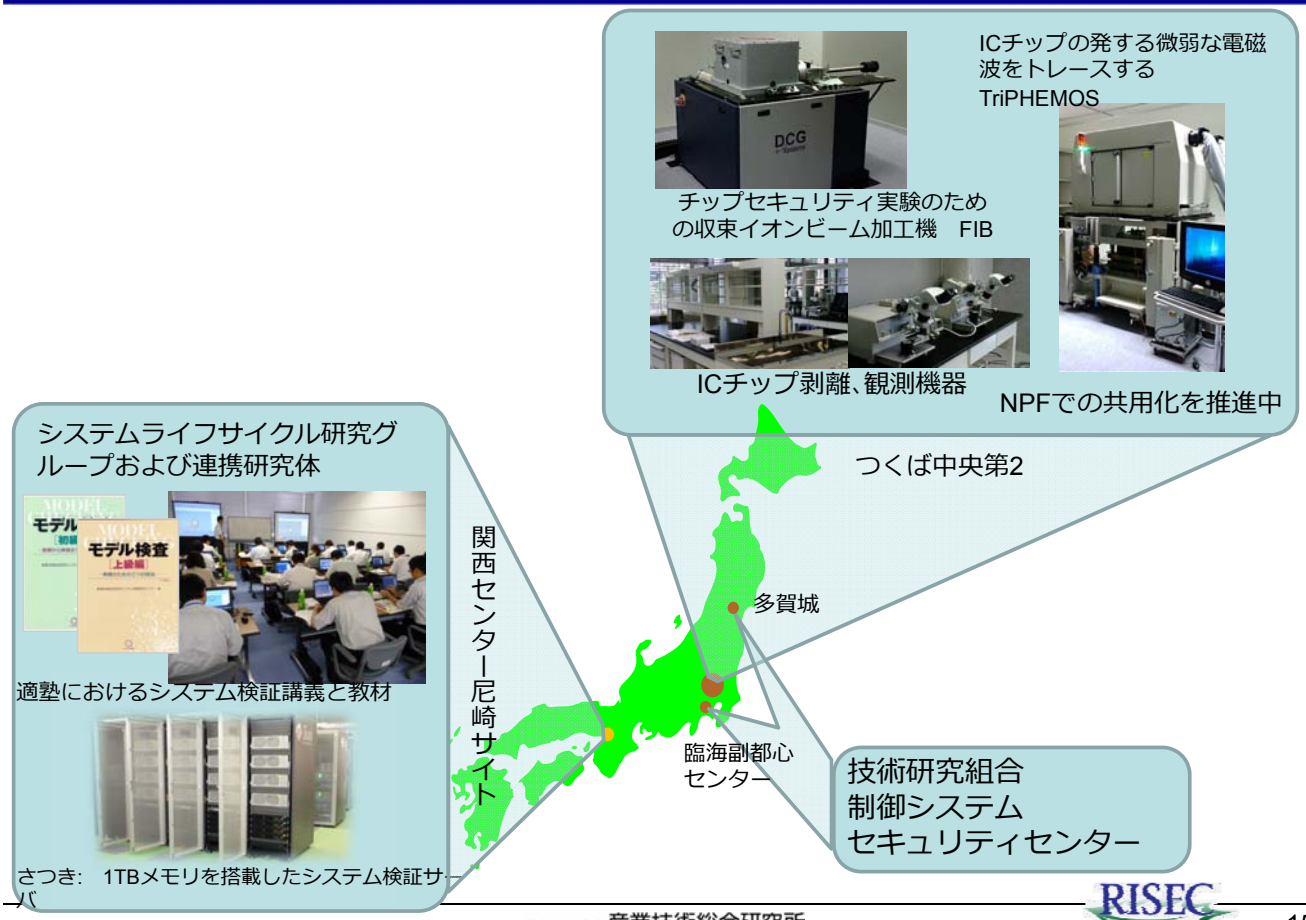
	対象領域	守る情報の性質	活動内容
ITサービス	クラウド、携帯電話やインターネットサービス、電子政府(情報漏洩)	機密性	•クラウドサービスのプライバシやトラスト、、ガイドラインや技術文書 •認証技術、鍵管理 •ヒューマンファクタ •高効率符号化 高木
制御システム	インフラ系、監視制御系、スマートグリッド、LSIチップ、(激甚化)	可用性	•重要インフラ制御系の高セキュア化 •制御ネットワークの侵入検知、防御技術 •ICチップのセキュリティ評価 古原
安全システム開発	組込機器、ソフトウェアの開発運用ライフサイクル(根本対策)	信頼性 完全性	•安全なソフトウェアの設計開発・テスト手法 •仕様記述から高信頼な実装の生成 •信頼性の評価、標準化 •仮想化によるマルウェア検出 大岩 北村
次世代システムセキュリティ	クラウドなど応用向き次世代暗号(次の脅威への備え)	機密性 可用性 完全性	•暗号の安全性証明・評価 •機能強化された次世代暗号 •コンテンツ配信における著作権保護 花岡

システム安全へのオールジャパンでの取り組み



RISEC

研究拠点と設備



ゲームチェンジは可能か？

技術を飛躍的に向上させれば、
防御側有利になるのだろうか？

他の情報系ではどうだろうか？

- 生命は、サイバーの大先輩
  - 生物は、DNAの乗り物
- 生命のセキュリティ戦略は？

http://www.free-desktop-backgrounds.net/Animals-wallpapers/Lion-wallpapers/Lion-and-zebra.html

なりすまし、フィッシング

托卵

http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0007725

ウグイス(親)　　カッコウ(子供)

http://www.pbs.org/wgbh/nova/sciencenow/0407/03-moth-06.html

DoS攻撃

イナゴの大群

http://www.ento.csiro.au/education/insects/orthoptera_families/acrididae.html

コウモリの大群

http://durangoherald.com/article/20120902/LIFESTYLE03/709029975/0/Lifestyle06/Endangered-bats?-Not-at-Carlsbad-Caverns#

峰球: ニホンミツバチは、スズメバチに襲われると、大勢で取り囲んで体を震わせ、40度近い熱で焼き殺す

http://hyhc72.blog48.fc2.com/blog-entry-846.html

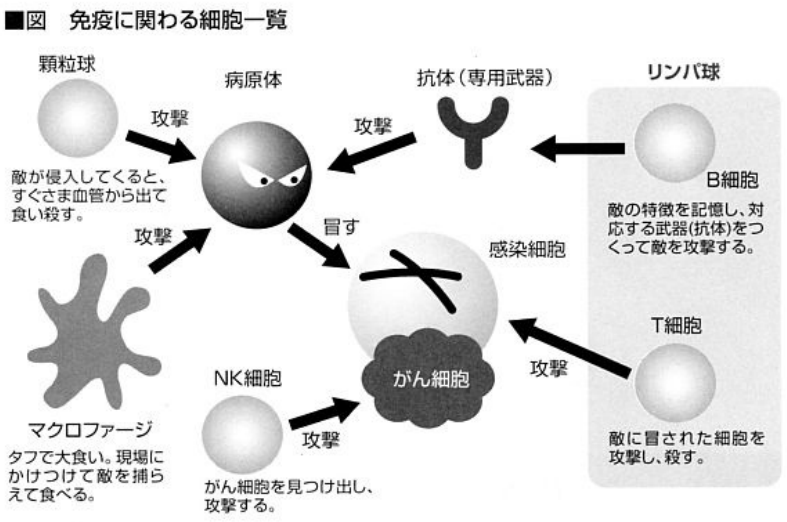
標的型攻撃、マルウェア

テッポウウオ
http://news.sciencemag.org/sciencenow/2004/09/07-01.html

http://amazingfactsoftheworlds.blogspot.jp/2011/12/king-cobra-snake-facts.html

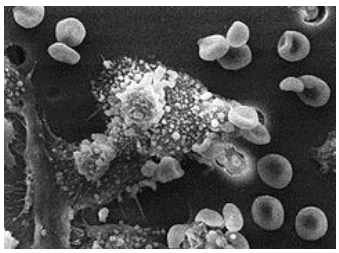
http://www.pbase.com/jeremy101/image/57977463

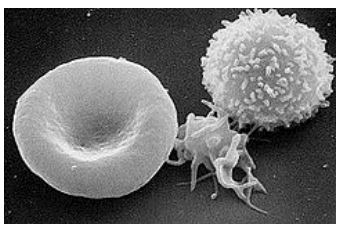
防御： 免疫系



http://www.zennyuren.or.jp/qa/wakaru50/q28.htm

出典:全国牛乳普及協会、牛乳の三次機能とQOL





http://ja.wikipedia.org/wiki/免疫系

防御： 擬態

クロアゲハ

ジャコウアゲハ
http://movie.geocities.jp/tom_kasa55/column224.html

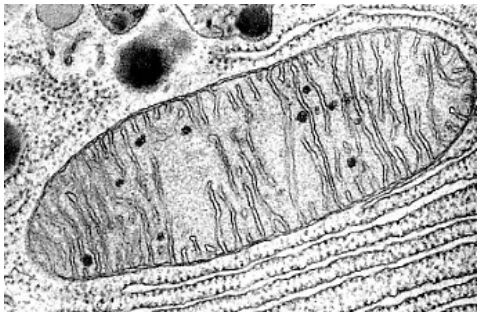
http://izismile.com/2009/10/23/amazing_natural_camouflage_18_pics.html

http://eco.goo.ne.jp/nature/unno/diary/200809/1221029216.html

生命型セキュリティ戦略との比較

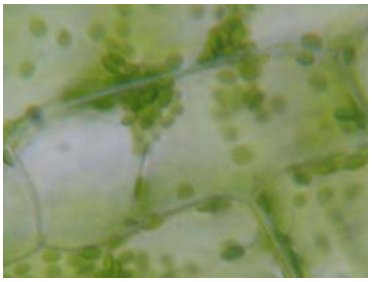
生命	サイバー
膜構造	ゾーンディフェンス
多細胞	冗長系、多重系
使い捨て	update
アポトーシス	システム検証
おとり　(トカゲのしっぽ)	honeypot
擬態	偽バナー、電子透かし
ニオイ付け	バイオメトリクス
免疫	ホワイトリスト
自己修復	エラー訂正符号

ウィルスとの共存



DON FAWCETT-KEITH R. PORTER/
PHOTO RESEARCHERS, INC.

ミトコンドリア
Mitochondria



葉緑体
chloroplast

http://mittu-3839.cocolog-nifty.com/blog/2006/06/post_68ad.html

多様性

- **多型　(血液型)**
  - **Win, mac, linux, Android, iOS, ,,,**
- **生物種**
  - **200万～1,000万～1億種**
- **大量絶滅での生存**
  - **2.5億年前の地殻変動、6500万年前の巨大隕石衝突**
- **多くの種の保存にはコストがかかる**

暗号

- 11年ゼミ、13年ゼミ、17年ゼミ
- ？？？

ゲームチェンジは可能か？

http://wellwire.com/health/sleep-health/when-the-zebra-rides-motorbikes-an-adrenal-story

- 生物のセキュリティ戦略を全部実施して、ようやく生態系の均衡が保てる
- 人間の知恵は、その均衡をくずし、多くの種を絶滅させるほどに強力
- サイバーでは、まず均衡に持ち込むために、生命系に学んでやるべきことはたくさんある

RISECと共に、世界のIT安全を目指しましょう

RISECとの連携の方法

- 共同研究
- プロジェクトの共同提案
- 連携大学院
- 学術振興会特別研究員

http://www.risec.aist.go.jp/
risec-liaison-ml@aist.go.jp
risec-recruit-ml@aist.go.jp
AISTオープンラボ 10/25-26

ご清聴ありがとうございました