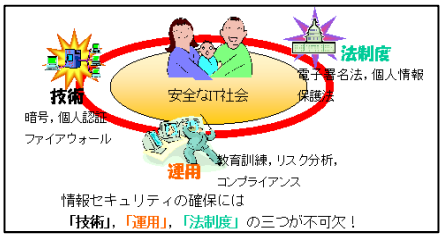
財団法人九州先端科学技術研究所

Institute of Systems, Information Technologies and Nanotechnologies (ISIT)

情報セキュリティ研究室

我々の生活の中でインターネットは大切な社会インフラであり，その安全を守るための情報セキュリティ技術は欠かすことができない．そこで本研究室では情報セキュリティ技術に関する研究と運用，法制度に関する調査活動を行っている．



研究室メンバー

研究室長：櫻井幸一（九州大学大学院システム情報科学研究院教授）

研究員：高橋健一，橋本康史，江藤文治

ホームページ：http://www.isit.or.jp/lab2/index.html

連絡先：isit-lab2@isit.or.jp

研究紹介

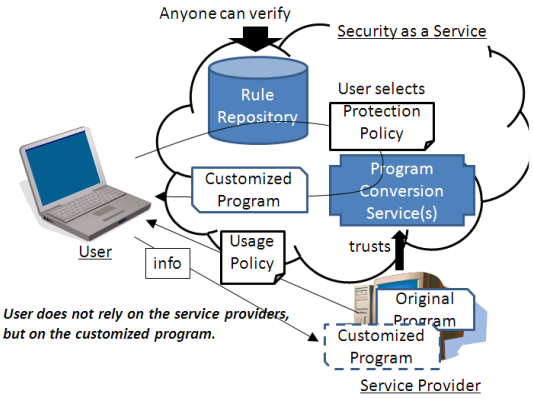
ユーザがカスタマイズ可能な個人情報保護実現に向けた研究（担当 高橋健一）

◆ インターネット上サービス利用に個人情報の提供が必要
（例．ユーザ登録，オンラインショッピング等）
- サービス提供者がどのようにユーザの情報を利用するのか？
- 目的外利用するかも → 情報漏洩等の原因に

◆ 情報の利用方法はサービス提供者に依存！
→ 情報の利用についてユーザ側の決定権がない！

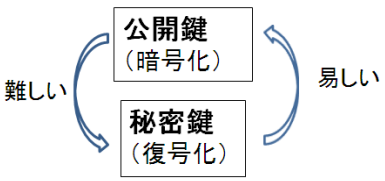
ユーザが安全だと思う方法で，ユーザが指定した方法で

◆ 個人情報処理方法をユーザが指定する方法が必要では？
- 自分自身で情報を保護するための方法が選択できる！



公開鍵暗号の研究 （担当 橋本康史）

◆ 公開鍵暗号方式
- 数学の一方的に困難な問題を使った暗号方式



例：RSA暗号 ・・・・「素因数分解問題」
p,q ； 素数、n = p × q ： 整数、
p,q → n ： 易しい
n → p,q ： 難しい

◆ 目標
- 既存の暗号方式の解析
- 安全で効率的な暗号方式の設計

◆ 成果
1. RSA暗号について
   - 特殊な条件下（素因子の部分情報が既知で秘密鍵が小さいとき、等）での解析
2. 多変数暗号（連立2次方程式を用いた暗号）について
   - 変数の個数が方程式の個数よりも多いときの方程式の解法
   - 2003年版UOV(署名方式の一種)の解析

セキュリティ評価を考慮した通信経路選択の研究 （担当 江藤文治）

◆通信システムのネットワーク経路選択〈現状〉
- 宛先までの経路の確保を通信パラメタに基づき要求
  宛先(IP addr.), Weight, 帯域, 遅延, 揺らぎ etc.
- NWのリソース使用状況，運用状況(輻輳/障害)
  を考慮し,パラメタ要求を満たす経路の中から選択

◆課題
- 選択経路のセキュリティを規定するパラメタは？
- 経路のセキュリティを考慮した選択は？
  選択経路のセキュリティのレベルは保証されない
  ⇒ [攻撃への耐性、攻撃検知の容易性 etc.]

◆提案
⇒経路のセキュリティを評価,高レベルの経路を選択