
暗号システムと人間

—人間が使うということによる問題点について—

土屋俊

(千葉大学)

ヒューマンクリプト？

- ユーザがコンピュータへのアクセスを安全にし
かも容易に実現するための暗号関連的技術
(個人認証技術およびその利用技術)
- ユーザが暗号・認証システムを容易に使える
ようにするヒューマンユーザインターフェイス
技術
- 暗号・認証システムがユーザの考えている通
りに機能していることを保証し、またそれを
ユーザに適切に表示する技術

背景

- 人間の日常生活における認知能力に関する研究(目撃証言研究など)
- 認知科学的ユーザインターフェイス技術
- CSCWなどのグループウェア技術
- 分散AI技術
- いわゆる社会技術
 - 社会制度、社会システム(法律、経済など)
 - 人間の意識、人間関係、信頼・信用に関する研究
 - 倫理綱領、運用ガイドラインの作成と運用の研究

人間の日常生活における認知能力

- 従来の実験室的研究への反省
- 実用的要請(目撃証言など)
- テーマ
 - 知覚
 - 記憶
 - 推論
 - 言語

(認知科学的) ユーザインターフェイス技術

- 間違えないためのインターフェイス
 - ドアノブの例
 - Direct manipulation
- 機器の表示インターフェイス
 - 間違えない手順
 - ビデオ予約システム
- 状況的推論
 - ゼロックスインターフェイス
 - 周辺の参加

グループウェア

- 共同作業環境の研究
 - エスノメソドロジー
 - CSCW (computer supported collaborative work)
 - グループウェア (Lotus Notes, etc)
- マルチエージェントシステムにおける情報交換のためのプロトコル
 - 情報内容
 - 情報機能 (speech acts etc)
- 「ここからの情報ならば信じてよい」

社会技術とは

- 同時進行的社会設計
- Social designとしての「社会技術」
- その対象
 - 法律、経済制度
 - 慣行、慣習、ポリシー、ガイドラインetc
 - 倫理、意識、考え方、態度
- 上記の具体的技術開発への反映

方法

- 人々の考え方、態度の調査
 - 定量より定性調査の重視
 - アンケート手法よりインタビューを重視する「深い調査」
- 実験的方法
 - 比較的大規模の社会実験
 - 行動科学、認知科学的実験室実験によるモデル設計
- シミュレーション
 - 意識や規範を組み込んだ社会・経済モデル
 - 意識や規範を反映したセキュリティ対策技術開発
- Request for Comments方式
 - 提案、提唱に対するパブリックコメントを求める (Web利用)

分野・テーマ

- 例

- 「情報セキュリティに関する人々の意識のデザイン」
- 「情報セキュリティに関するポリシーとそのバランスのデザイン」
- 「セキュアな世界実現のための社会モデルデザイン (社会レベル / 1 社会の枠を越えた国際レベル)」
- 「情報セキュリティにおけるヒューマンインターフェイスのデザイン」
- 「情報化社会の人間活動予測に基づくセキュリティ対策モデルのデザイン」

予想される成果

- 情報インフラを信頼し、安心して社会生活を営めるようになる(個人レベル)チェックリスト
- セキュリティ意識が向上する(個人レベル)
- 不要な社会的利害対立に巻き込まれることなく情報技術を活用して、設立の目的を遂行できる(団体レベル)(企業は利益を、公共団体は公共サービスを)情報管理、公開、技術利用ポリシー、教育カリキュラム・方法・教材
- 社会的カタストロフィの回避(国レベル)

文理融合の新しい方法論

- 情報社会を捉える、国際的に通用する新しい概念の提唱
- それにもとづくセキュリティ概念、セキュリティ技術の開発と、セキュリティシステムデザインへの反映
- 英語による概念の発表（海外に向けた発信）
- 多様な分野の若手研究者を中心にした取り組み
 - 情報学(計算機科学、人工知能、ネットワークなど)
 - 社会科学(法律、経済、社会学など)
 - 人文科学(哲学、倫理学、言語学、図書館学など)
 - 認知科学(心理学、社会心理学、人類学など)
- できるだけ同じ場所で常に話しあえる環境
- 成果の随時公開、コメント受付、随時修正