研 究 発 表 会 実 施 概 要

１　日　時　　平成１７年１２月７日（水）　１４時３０分～

２　場　所　　１００周年記念会館　第２会議室

３　内　容

（１）　研究発表（14:30～15:10）

・森岡　孝二　経済学部教授

発表テーマ「ニューエコノミーと過重労働

――『働きすぎの時代』（岩波新書）を著して――」　資料１

・小谷　賢太郎　工学部助教授

発表テーマ「認証システムのセキュリティ向上を目指して」　資料２

（２）　質疑応答（15:10～15:30）

４　大学側出席者

広兼道幸学長補佐、森岡孝二経済学部教授、小谷賢太郎工学部助教授、他

５　参考資料

（１）第１０回先端科学技術シンポジウム リーフレット

（２）第３回ソシオネットワーク戦略研究国際会議・

第１回政策グリッドコンピューティング実験センター国際会議　チラシ

（３）特別公開講座　リーフレット

（４）経済・政治研究所　法学研究所公開セミナー　チラシ

（５）第１６７回経済・政治研究所公開講座　チラシ

（６）関西大学ＦＤフォーラム Vol.10

（７）ニューズレター／ＲＥＥＤ №.6

（８）関西大学通信 第 330 号

（９）電子情報学会　情報・システムソサイエティ誌(抜粋)

以　上

【テーマと概要】

ニューエコノミーと過重労働

――『働きすぎの時代』（岩波新書）を著して――

経済学部教授　森岡孝二

【概　要】

厚生労働省『毎月勤労統計調査』によれば、2004 年の日本の１人平均年間労働時間は 1816 時間であった。これを額面通りにとれば、1988 年に発表された「年間 1800 労働時間」という政府の時短計画は、目標年次から 10 年以上遅れてではあるが、いまや達成されたことになる。1992 年に制定された「時短促進法」が先の国会で廃止されたことも、それと符合するように思われる。

にもかかわらず、なぜ、いま、働きすぎを問題にするのか。実は、年間 1800 時間の達成には二つのからくりがある。第一に、この数字は、総務省『労働力調査』から見て、１人当たり年間約 350 時間にも及ぶと推計される「サービス残業」（賃金不払残業）を含んでいない。第二に、この間の統計上の労働時間の短縮は、パート・アルバイトなどの短時間労働者の増大がもたらした平均のマジックにすぎない。

働きすぎは強まってさえおり､フルタイムの 30 代男性の４人に１人は週 60 時間(年間 3000 時間）以上働いている。平均でも週 50 時間に上る。近年では採用抑制やリストラによって人員が減らされながら仕事量が増え、過重労働やストレスによる健康障害やメンタルヘルス問題が深刻化し、過労死や過労自殺やうつ病が広がっている。

今日では働きすぎは日本だけの問題ではない。アメリカでもイギリスでも、10 年ほど前までは日本の風土病のように言われていた過労死が起きている。時短先進国として知られる独仏や北欧でも、労働時間の逆流が生じている。拙著では、世界に広がるこうした働きすぎの背景を、「グローバル資本主義」「情報資本主義」「消費資本主義」「フリーター資本主義」をキーワードに考察し、働きすぎにブレーキをかけ、まっとうな働き方ができる社会を創っていくために、いま何が必要なのかを提起した。

認証システムのセキュリティ向上を目指して

工学部助教授　小谷賢太郎

【概　要】

近年インターネットの普及や情報技術の向上により、インターネットを用いた商取引や、IC カードの普及といった利便性が高まる一方で、認証セキュリティ技術の向上が要求されている。指紋認証に代表される身体的な特徴を用いたバイオメトリクス技術は高い認証精度を誇り、多方面で利用されている。しかしながら一方で、身体的特徴は生涯不変な情報のため、特徴情報が漏洩すると再登録が出来なくなったり、指紋情報を登録することに不快感を示す人も少なくない。そこで我々の研究室では特に、人間の行動的特徴を用いたバイオメトリクス認証技術をベースとして、ATM などの認証に用いられている暗証番号入力時のセキュリティや、パソコンからの電子商取引へのログイン時のセキュリティといった、認証情報の漏洩が発生した際に、「成りすまし」行為からセキュリティを確保する技術の開発を進めている。本報告では我々の研究室においておこなっているいくつかの認証システムのセキュリティ向上を目指した取り組みについて紹介する。

図1　半導体感圧センサを用いたテンキーパネル

暗証番号入力時の指先の押圧力を計測し、認証情報として付加することにより、暗証番号入力時の動画像が撮影などにより漏洩しても、視覚的には変化を捉えにくい堅牢な本人識別能力を維持することが出来る。

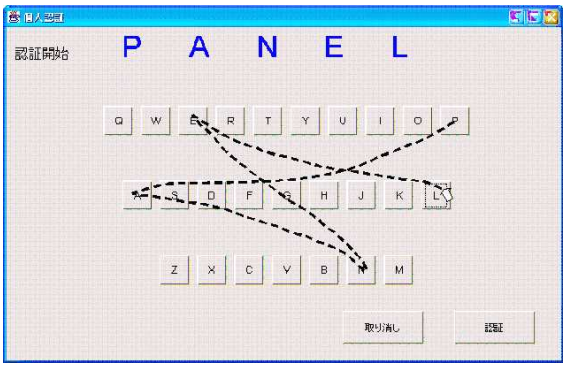

図 2　ソフトキーボード上のマウス操作軌跡

パスワード入力時のマウス操作軌跡（点線；本来は不可視）を用いたバイオメトリクス認証システム。パスワードが漏洩してもユーザのマウス操作の「くせ」によって本人の識別が可能。指紋読み取りなどの特別の入力装置を必要とせずネットワークバンキングなどのセキュリティ強化といった応用が可能である。