

情報セキュリティ研究室

より安全かつ
より便利な
情報活用の
実現を目指して



稲葉宏幸 教授
【情報工学・人間科学系】

【経歴】
1992年04月-
京都工芸繊維大学 助手
2000年04月-
京都工芸繊維大学 助教授
2007年04月-
京都工芸繊維大学 准教授
2010年03月-
京都工芸繊維大学 教授

【研究分野】
情報セキュリティ、プライバシー保護、
電子透かし、ネットワークセキュリティ、個人認証

研究室探訪

情報セキュリティ
研究室

【研究概要】
暗号技術等をベースとする
情報セキュリティ技術を活用し、
安全な情報システムの提案を行っています。
主な例としては、
写真や映像等のデジタルコンテンツの
著作権を保護する電子透かし技術や、
なりすましや盗み見に強い
個人認証システムの開発などがあります。

スマートフォンやPCを開く時、webサービスを利用する時など
今や私たちはさまざまな場面でパスワードを利用しています。
そうした情報セキュリティに関する技術は
現代に欠かせないものであり、今なお進化し続けています。
その先端を行く情報セキュリティ研究室の活動に迫りました。

パスワードに代わる 新たな認証方式を探る

最近では至るところで耳にする「情報セキュリティ」という言葉。特にこの1～2年は新型コロナウイルスの影響によるリモートワークの普及などもあり、社会的な注目度がさらにアップしています。そうした情報セキュリティ技術の中で、私たちの生活に最も身近なのが「個人認証」です。「PCやスマートフォンは、操作している人が本人であるかを確認しないと使えません。その仕組みが個人認証です。認証がしっかりできていないと、なりすましのような問題が起こってきます」。そう話すのは、情報セキュリティ研究室の稲葉宏幸先生。この研究室では、新たな個人認証方式の開発に取り組んでいます。「最も一般的な認証方式としてはパスワードがあります。パスワードは分かりやすく、コストもそれほど高くないのでよく使われていますが、問題も多く知られています。その一つが『忘れてしまう』ということ。忘れるのを嫌がって簡単なパスワードを設定した結果、文字列を推測されてしまい、不正アクセスにつながったという被害が多く報告されています。そこで、最近ではパスワードを使わない認証方式もどんどん出てきています。スマートフォンで顔認証や指紋認証を使ったことがある方も多いのではないのでしょうか。この研究室では新しい認証方式として、画像を使ったものを検討しています」

そう言うと、先生は認証に用いる画面（Fig.2）を見せながら次のように説明してくれました。「画面にはこうしたカラーパネルの画像が表示されます。この背景配列部分のタイトルは指でスライド可能です。それで、あらかじめ決められたルールに従って背景配列をスライドさせ、パスワード文字に合わせることでパスワードの入力ができるようになっています。この方式を使うと、誰かがインターネットを盗聴していたり、あるいはスマホで入力している様子を後ろからこっそりのぞいていたりしても、どの文字に合わせたのかは本人以外分かりません。このように、盗聴やのぞき見への耐性を持つ個人認証の方式を考えています」。新しい認証方式を考える際には、どのようなポイントが重要になってくるのでしょうか。「まず意識しているのは利便

性です。ただ利便性は大事ですが、その点を重視するあまり安全性がおざなりになってしまっ
ては元も子もありません。そここのバランスが難しいですね」

そうして利便性について考え抜いた結果、先生は「何もしなくてもいい」という方式を思い付いたといいます。「何もしない」とはいったいどういうことでしょうか。「まず申し上げておくと、この方式も安全性は確保できるものとなっています。どのようなアイデアかという、周囲の人の協力を得て認証を行うという仕組みです。例えば研究室の仲間や、家族と一緒にいるとしましょう。そのような状況で認証が必要になった際、のぞき見している人や怪しい人が周囲にいれば気付くはず。従って、周りにちゃんと人がいて周囲に注意を払っているのであれば、その状況を認証クリアの条件にできるのではと考えました。具体的な仕組みとしては、スマートフォンのBluetooth機能、近距離無線通信を活用します。ある人が認証したいとなった時に、その人のスマートフォンから周囲の人のスマートフォンへと自動的にリクエストが送られます。それに対して周囲の人が返事を返すことで、認証のための合言葉のようなものが作成され、認証を行うといったイメージです。すると基本的に利用者は何もしなくてもよくて、周りに友人や家族がいれば認証ができる形になります」

この認証方式の応用イメージについて、先生は次のような話をしてくださいました。「最近ではデジタル遺産の相続が問題になっています。例えばネットバンクに入れたお金。利用者本人が病気や事故で突然お亡くなりになってしまった場合、アクセスができなくなり、引き出しの手続きなどが不可能になってしまいます。そうした時に先ほどの方式を使えば、本人のスマホを用意して周囲に家族がいる状況を作ることで、認証が可能になるはず。本来の認証とは少し意味が違ってもいいかもしれませんが、そういった応用もあるんじゃないかなと考えています」

デジタル時代に 対応した研究は他にも

情報セキュリティ研究室で行われているのは個人認証の研究だけではなく、「電子透



Fig.1——ディスカッションを重ねてアイデアを改良していく



Fig.2——カラーパネルを用いた独自の認証方式



Fig.3——研究室では課題発見力を重視

かし」もターゲットの一つです。紙幣には偽造を防ぐための透かしが入っていますが、まさにそのデジタル版といえます。「電子透かしは主に、いわゆるデジタル著作物の著作権を保護する目的で使われます。デジタルコンテンツは簡単にコピーできるため、不正な利用や複製を防ぐのは困難です。もちろんコピーライト表示は入れておくと思いますが、その部分だけ消してしまうことも容易にできます。そこで、人間の目には全く分からないけれども、特殊な方法でデータを復号すると著作権情報が分かるような仕組みができました。それが電子透かしです」。人間の目では分からないとのことですが、どのように透かしを入れ、どのように情報を読み取るのでしょうか。「さまざまな方式がありますが、最近検討しているのは数学的な技術を用いて画像の幾何学的構造を検出し、情報を取り出すというものです。例え

ば画像内に輪っかのようにになっている部分があるとしたら、その輪っかの分布で透かしの情報を表すようなイメージです。この方法を採用すると、画像の明るさが変わっていたり、拡大縮小されていたりしても情報はそのまま残ります。そのため、改ざんに強い性質を持つことが予想されます」。透かしには著作権情報の他に売買履歴などの情報も入れることができ、万一不正利用があった場合にも追跡が可能になるといいます。デジタルコンテンツが急速に増え続ける世の中で、より重要性を増す技術となりそうです。

デジタル化時代を見据え、 さらなる研究の深化を

最後に、研究の面白さや今後の展望についても語っていただきました。「日本では今後どん

どんDX（デジタルトランスフォーメーション）*が進んでいくでしょう。その時に情報セキュリティ対策をきちんとしていないと足元をすくわれる形になってしまいますので、この研究の社会的意義は非常に大きいと思います。また、情報セキュリティは守りの技術のように捉えられがちですが、この技術を活用することで新しいサービスを生み出せる可能性もあります。技術開発を行うと同時に、情報セキュリティの正しい理解を広めるための取り組みも進めていきたいと考えています」

*企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを軸に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

引用元：DX推進ガイドライン（経済産業省）