IMIT CHIBA UNIVERSITY Institute of Media and Information Technology

News letter

総合メディア基盤センター

Vol.7, No.1, 2011

最大のセキュリティホールは人間。それを認識してもらいたい

多田 充 准教授

2月に開催された総合メディア基盤センター主催する第2回シンポジウム「情報セキュリティ技術の恩恵」。第1回に続き好評を博したこのシンポジウムのご担当者であり、情報科学がご専門の多田 充准教授にご登場願いました。シンポジウムやご専門の研究を通して、現代の情報セキュリティに対する意識の持ちようやその重要性などについて、メッセージをいただきました。

産学お互いが学び合い、幅広い知識を得る機会としても有意義だったシンポジウム

ーシンポジウムはいかがでしたか。

今回のシンポジウムは、総合メディア基盤センターの企画としては第2回になります。第1回は古森教授が担当された「ラムダ計算／部分構造論理 その歴史と展望」というものでした。今回は私が担当しましたので、専門分野である情報セキュリティに関するものとなりました。

ー企業から講演者を招いた点が興味深いと思いますが、それぞれどのようなお話をされたのでしょうか。

1日めのKDDIさんは電子的著作物に対する著作権保護技術。富士通さんがウェブアプリケーションに関するセキュリティ検査技術、日立製作所さんがハッシュ関数の安全性と日立提案方式「Luffa」の紹介。2日めのセコムさんはクラウド時代のデータセンターのセキュリティと医療情報の外部保存に関する制度・安全管理技術。三菱電機さんはブロック暗号技術とその安全性の考え方について。そして最後に大学から、情報セキュリティ委員長をしておられる石井徹哉先生が「デジタル・フォレンジクス」について講演しました。

ー聴講者の反応はいかがでしたか。

おしなべて好評で、どの講演にも一定数の聴講がありましたね。特にどれが、というのではなく、皆わかりやすく、面白かったという反応でした。ただ、講演者の間では、石井先生の「デジタル・フォレンジクス」について考えさせられるという声がありました。デジタル犯罪をテーマとしているので、企業側とすれば、開発した技術が悪用された時に法律でどう判断されるのか、関心が高いところですので。

ー企業の方に講演していただいた意義、効果は何でしょうか。

2つの側面があると思います。学生には、企業が実際にどんな研究を行っているのか知って、幅広い知識を得てほしかったですし、企業としては自分の研究を紹介したいという思いがありますので、それに応えることができたと思います。

ーこのシンポジウムを通じて、最も伝えたい、知ってほしいと思ったことはどんな点でしょうか。

一般のユーザーは情報セキュリティについてなかなか意識が進まないという現状があります。普段使っているアプリケーションの中にはすでにセキュリティが考えられているものもあるので、ユーザーが意識していないところで情報セキュリティが働いていることを知ってほしかった。それから、事故が起ってから初めて考え始めるということが多いので、事前に防ぐということを意識してほしかったのです。技術は出来上がっているものなので、一番の問題は使う人間なのだということ。情報漏洩のニュースが多いですが、その原因の多くは人間の不注意です。

ー現代の情報セキュリティを取り巻く課題とは、何でしょうか。

最大の課題は、ユーザーが「自分は大丈夫」と過信していることだと思います。自動車事故と同じですね。でも思わぬところで事故は起ってしまうものだということを、わかってほしいですね。

システムの恩恵を受けるのなら、ある程度は知る必要がある

ー多田先生のご研究である「相互匿名認証」について、かいつまんでお教え下さい。

認証を行う場合、そのユーザーに権限があることだけわかれば、その人が誰であるかを問わないことが多い。「グループ署名」というグループ内匿名署名方式があり，これは一方向的な匿名性を保証しますが、「相互匿名認証」はその匿名性を双方向にしたものです。たとえば「Secret Handshake」という、二者が同一グループである時だけ認証が成功し、そうでなければ互いに誰であるかはもちろん、そのグループすら秘匿になる方式などです。この構成方法や安全性、効率を評価する研究です。

ーもうひとつの「次世代公開暗号系」についてもお願いします。

現在私たちが使っている公開鍵暗号系は主にRSAという方式で、素因数分解の難しさを利用しています。たとえば15という数字は5×3などと簡単にわかりますが、桁数が多くなるとコンピュータでも計算に数千億年とか膨大な時間がかかり事実上計算不可能になる。ただ、現在のコンピュータは古典力学の原理で動いていますが、「量子計算」という量子力学に基づく計算が実現すれば、素因数分解は一瞬で計算できることがすでに証明されていて、そのときRSAの安全性は保たれなくなります。したがって、量子計算に対しても安全性を保つ仕組みを考えなくてはならないのです。

ー先生のご研究が最終的に目指すところとは何でしょうか。

公開鍵暗号系は、主に「整数論」「計算量理論」を土台としていますが、私はその土台となる分野で真理を追究したいと思っています。その結果がいずれ、実際の情報技術に利用される日が来るのではないかと。未来に向けての研究ですね。

ー一般のネットユーザーに向けて、ネット上のセキュリティに関して、気をつけてほしいと思うことは。

一般の人が最も使うアプリケーションは、ウェブ、メールですよね。メールはいわばハガキのようなもの。見ようと思えば誰でも見ることができるものなので、機密性が要求されることはメールでは流さない。また、ウェブは「なりすまし」が可能です。フィッシング詐欺などがこの手口ですが、あるサイトに似せたページは簡単に作れる。そういうことを知っておくだけでも違うと思います。

繰り返しになりますが、最大のセキュリティホールは人間であること、これを自覚してほしいと思います。昔は見るだけだったウェブも、ブログやショッピングなど、ユーザ自身が情報を発信することが多くなった。その情報はどこへ行くのか。もし間違えると…。システムの利便性や恩恵を受けるなら、ある程度は情報セキュリティについて知らなければいけないと思いますね。

編集・発行 千葉大学総合メディア基盤センター 〒263-8522 千葉市稲毛区弥生町1-33
Tel: 043-290-3535 Fax: 043-290-3518 http://www.imit.chiba-u.ac.jp/index.html