研究所の姿

NTT情報流通プラットフォーム研究所

安心・安全のセキュリティ技術を開発し信頼性の高いネットワークの構築を目指す

NTT情報流通プラットフォーム研究所
後藤厚宏所長

NTT情報流通プラットフォーム研究所（PF研）は武蔵野研究開発センタ内にあり，情報流通基盤総合研究所の一角を占めています．PF研が行うのはネットワーク社会に欠かせないセキュリティ技術の研究開発．同研究所の後藤厚宏所長を訪ね，最新の技術等について話を伺いました．

研究所の位置付けと役割について

◆研究所の位置付けと役割を教えてください．

PF研は，情報流通基盤総合研究所の傘下にあります．主要なミッションとしては，情報流通の基盤にかかわるネットワーク技術やセキュリティに関する技術の研究開発を行っています．ネットワークの機能を活かして，安心・安全なサービスを展開するために必要な機能や全体の仕組みを技術として提供しています．

安心・安全というキーワードをベースとしている技術は大きく，3つに分類されます．まずはいわゆる暗号技術です．これはデータの暗号化を行い，情報漏洩を防ぐものです．次にネットワークを安心・安全に運用するためのネットワークセキュリティ技術です．さらに，サービス提供者が横断的に必要となる基盤・機能をプラットフォーム化する技術です．これら3つの技術をうまく組み合わせ，安心・安全・便利な各種情報流通ネットワークサービスを提供していくのがPF研の役割です．

◆代表的な技術にはどのようなものがありますか？

2000年にNTTと三菱電機が共同で「Camellia」を開発しました(1)．Camelliaは，共通鍵を使用する暗号化の国産技術で，利用環境に応じて，高速で柔軟性に富んだ実装が可能であるため，搭載メモリが少ないICカードやUSB等の可搬性のある媒体の保護にも適しています．

本技術は基本特許を無償化しています．これは，国内外のさまざまな製品やサービスに広く利用できる環境づくりに貢献し，暗号技術の普及・促進により，低コストで安全な高度情報流通社会の実現に向けて主導的役割を果たすためです．また，技術的にも「米国政府標準暗号AESと多くの点で同等の安全性と性能を有している」と国際的にも評価されており，Linux等のオープンなOSやMozilla Firefoxといったフリーのブラウザソフトウェア等に広く採用されています．

ICTに見る光と影

◆いわゆるICTは，我々に多くの利便性をもたらしましたが，一方で，弊害もありますね．

ICTは基盤技術として非常に便利な反面，それを悪用し，犯罪につながるような行為や事故が近年，多発しています．例えば，官公庁の重要なシステムをねらったハッカー行為やネットショッピングで他人になりすましたりするといった悪質な行為が増加し，年々手口も巧妙化しています．

ネットワークセキュリティにおいては，銀行が開設しているホームページを詐称して，本物に見せかけた偽のホームページに顧客を呼び込み，口座の暗証番号や個人情報へのアクセスに必要なID・パスワードを盗み出すといった「フィッシング」等の手口が後を絶ちません．

また，送られてくるメールのみならず，ホームページ，さらにフリーで配布されているソフトウェアの中にもウイルスが仕込まれている場合があり，油断できません．

◆PF研ではそれら「影」の部分にどのように対処しているのですか？

私どもの研究所では，単にウイルスを駆除するためのアンチウイルスソフトをつくるということは行っていませんが，実際に出回っているウイルスにどのようなリスクが潜んでいるかということを把握するのに必要な分析技術や，ネットワーク上のさまざまな攻撃に対する防御技術の開発にも取り組んでいます．

また，ネットワークを利用する上で発生するリスクを未然に防ぐためには，内外のネットワーク関係者との協力が必要です．そのために，PF研が主体となり，国内の企業や海外のネットワーク関連情報を収集している企業とも連携を進めています．さらに，ネットワークセキュリティの保持や，情報漏洩といった問題に対し，どのようにセキュリティを確保していくのかという，体制や運用といったセキュリティマネジメントについての研究も行っています．

これら以外にも，安心・安全で快適・便利なサービスを数多く創出できるサービス基盤の構築を目指し，そのための基礎となる暗号アルゴリズムから認証・ID連携などの研究開発や，IPv6といった次世代インターネット技術の研究開発に取り組んでいます．

ネットワーク社会を支える新しい認証方式

◆認証をより簡便に行い，かつ，強力なものにすることができるのでしょうか．

現状，インターネットでよく利用される認証方法に，ID・パスワードでログインするやり方があります．けれども，これらは他人に使われてしまう可能性がありますので，１回のログインでは不十分で，実際には送金する等の場面で，もう一度別のID・パスワードを入れ，認証を強化することが必要です．

PF研では，何度もユーザの手を煩わせることなく，より簡単に，信頼性・安全性を高めることが可能な認証方式についての研究開発も進めています．

例えば，各家庭のPCから，お客さまがネットワーク上のサービスにログインしたときに，どの回線が使われているかを識別する技術があります．この場合，ID・パスワードだけでなく，使用している回線が一致しなければ認証できない仕組みですから，ID・パスワードが盗まれたとしても，本来それが属している所の回線を識別できないとなると，例えばインターネット経由でオンライン銀行から預金を引き出そうとしてもできないことになります．

このように，ID・パスワードの認証と回線の識別を同時に行い，セキュリティを強化する，ということについても研究が進んでいます．もちろん，前述の技術は家庭からアクセスすることを想定していますから，外出先や移動先で認証を得たい場合等，近年，利用が増加しているモバイルの時代に見合った認証識別の技術も，今後は必要になるでしょう．

◆新手のウイルスやネットワークの攻撃に先行して手を打ち，攻撃そのものをなくすことはできないのでしょうか．

可能かもしれませんが，それは目指すべきことではないかもしれません．と言いますのは，まず，すべてのリスクを遮断するシステムは，ユーザにとり，大変使い勝手が悪く，不便な物になる可能性があるからです．

例えば今，社会の犯罪や交通事故がゼロになっているかといいますと，そうではありません．それらをなくすためには，国民の２人に１人位の警官を増やすことが必要になるかもしれません．そうしますと，莫大なコストがかかることになります．交通事故も，車がなければ起こらなくなりますが，果たしてそれができるでしょうか．

システムも同様で，セキュリティとコストのバランスをみながら，ちょうどよいところで，安心・安全を確保することが期待されているのではないでしょうか．もちろん，ウイルスをつくってばらまいても，その手口に引っかかる人がいなくなれば，今度はウイルスをつくる人が，そのことに魅力を感じなくなり，結果的に，ウイルスが減少する，ということになる可能性はあると思います．

人間社会として，どれくらいのところが良いのか，ということに関しては，社会的・心理的，また，法律・社会的な制度に照らし合わせるなど，多面的に考える必要があるでしょう．セキュリティの問題は，最後には必ず人や，個人情報保護法といった法律等の社会基盤ともかかわってくることでもあります．それらの部分とバランスを保ち，システムのセキュリティを確保することが大切であると考えています．

世界中のウイルス情報や暗号化技術についての情報の収集がかかせない

◆常にセキュリティ技術の改良を重ねなければならない中で，どのような課題があるのでしょうか．

例えば暗号化技術にもいろいろなかたちがあるということ，また，世の中のさまざまなシステムにそうした技術が組み込まれていることから，それらをすべて把握することは困難で，加えて，そうした技術がどのようにシステムやネットワークに影響しているのかということの情報が集まりにくくなっている側面があります．

しかし，セキュリティ技術に改良を加えるためには，それらのどこを，どのように改良したらよいのか，また，新たに投入

◆所長の横顔


後藤厚宏所長

○これまでのご経歴をお聞かせください．

私は1984年の入社です．民営化のちょうど１年前のことでした．最初に配属されたのは武蔵野にある，情報通信基礎研究部です．入社して間もなく，国のプロジェクトで第五世代コンピュータの開発を行うICOT（新世代コンピュータ開発機構）に出向しました．そこで，並列マシン開発や知識情報システムに関するさまざまなテーマの研究をしていました．

1990年代には米国のシリコンバレーで研究所分室を開設し，そこを拠点にスタンフォード大学との共同研究をスタートさせました．帰国後，マルチフィードというベンチャー事業の立ち上げに携わりました．2000年代に入り，ユビキタスやセキュリティ関連のプロジェクトマネジメントにかかわるようになり，2007年７月にPF研の所長に就任しました．

○所長にとり，研究の醍醐味とは？

研究というより，仕事の醍醐味と申し上げた方がよいと思いますが，「モノ」や「技術」，あるいは「組織」や「ビジネス」にしろ，何かをつくり上げている，という実感を持てることが嬉しいと感じています．

例えば並列マシンの開発ではLSIに組み込まれている仕組みの部分について，自分で設計をし，シミュレーションで評価し，論文を書き，かつ，製造し，稼働すると大変嬉しいものがありますし，同様に，会社の立ち上げでは株主を説得して回るといったことの苦労は，寝る暇のないほど忙しい思いもしますが，会社が立ち上がったときの満足感・達成感は格別です．モノづくりに限らず，そこが仕事の醍醐味なのではないでしょうか．

○所員の方々とは日々どのように接していらっしゃいますか？

PF研の所員は，技術的な研究の深さに加え，社会的な視野が広く，バランスの取れた人が多いと感じています．専門領域と，それをビジネス化した場合にどうなるか，また，社会的な影響がどうなるのかといったことの興味を持っているようです．

社会的な勉強というのは，特に私が強制しているわけではなく，所員が自主的に行っていると思います．もちろん，私自身は機会があれば，積極的に話しかけるようにしていますし，相談を持ちかけられれば，それにも乗りますし，助言もします．また，コンピュータネットワークの学会や法律の研究会等にも参加することを勧めることもあります．

○ご趣味は何ですか？

ロードバイクにはまっています．これは高速走行用の自転車のことで，２年ほど前から乗り始めました．多摩川沿いのサイクリングロードが五日市の辺りまで延びていますが，それを１日２時間ほど，天気の良い日には平均，往復で40～50 kmほど走ります．最近話題のメタボリック対策にもなりますし，心地よい疲労感があり，気持ちの良いものです．帰宅して飲むビールの味がこたえられません．

ほとんど１人で乗りますが，時々，自転車を購入したショップのイベントに参加して，仲間と「朝食ライディング」をして横浜の中華街に行き，朝粥を食べたり，築地で刺身定食を食べたりしています．所内でロードバイクをやっている者もいて，ハワイのオアフ島や佐渡島一周といったイベントに参加しているようです．私も誘ってほしいのですが（笑）．

する技術をどこに組み込めばよいのかという情報が必要で，それらの情報を常に把握できる仕組みや情報収集の体制が必要であると痛感しています．

◆今後の取り組みについて，お聞かせください．

まずNGNの本格商用化に向けた取り組みを推進していきます．NTTグループのみならず，さまざまな事業者がさまざまなサービスを展開しますが，それらのサービスをセキュリティ面で，いかに支援するか，PF研では暗号・認証による，安心・安全なネットワークやサービスを提供できるよう，尽力しています．

今後もPF研が行う研究開発の方針に，変わりはありません．常に改良を重ね，より安全で，より，新しいウイルスや攻撃に強いもの，また，ネットワーク等の脆弱性をねらうようなウイルスをより迅速に，簡単に見つけることのできる技術を研究するとともに，より使いやすく，より利便性が高く，強化されたセキュリティ技術について研究を継続します．

（インタビュー：松本美菜）

■参考文献

⑴ 神田：“国産暗号Camelliaの普及に向けた取り組み，”NTT技術ジャーナル，Vol.17，No.12，pp. 20-23，2005.

◆我が所のイチ押し

■ネットワークセキュリティに関する研究開発

図1はPF研の代表的な研究である，ネットワークセキュリティ技術です．トラヒックの異常やウイルスの検知からネットワークの事故，関係各所への連絡や暫定的な処置，また，恒常的な対策，さらにはウイルスやネットワークの脆弱性の分析・研究等について，PDCAサイクルの中で関係各社と連携しながら行っています．

■情報セキュリティに関する研究開発

図2はPF研が行う暗号技術や情報漏洩防止技術等，情報セキュリティに関する研究開発のアプローチ図です．ネットワークを安心・安全に利用するために，こうした技術が欠かせません．

本文で紹介されている暗号化技術「Camellia」もその1つです．本技術は国産としては初めて，インターネットの標準暗号として，また，ISO/IEC国際標準暗号として採用されました．

さて，NTTのホームページによれば，「Camellia」という名称は花の「椿」から採っているそうです．学名は「カメリア・ジャポニカ」．本暗号化技術が国産ですから，日本原産の植物名は，ぴったりのネーミングですね．

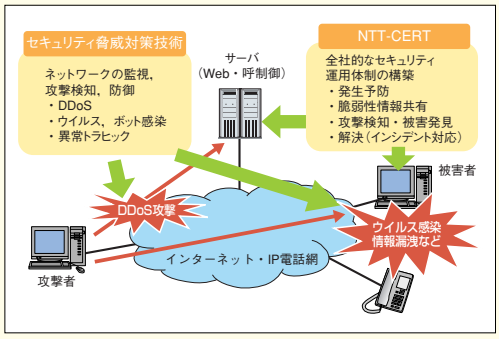

図1　ネットワークセキュリティに関する研究開発

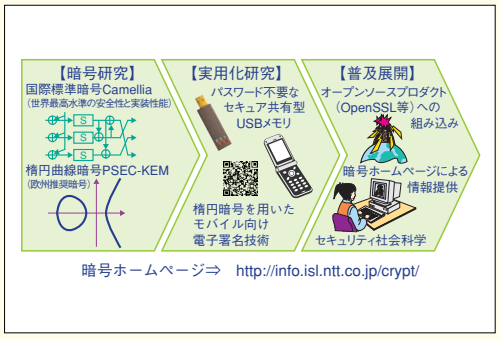

図2　情報セキュリティに関する研究開発

◆暗号化技術の大家がPF研に

NTTはグループ内で2007年4月から正式にフェロー制度を導入しています．この「フェロー」という称号は，優れた功績があり，世界的にも認められている方にのみ，与えられます．

制度化されてからフェローに任命されたのはCS研の守谷健弘氏，そしてPF研に現職で在任しておられる岡本龍明氏の2名です．岡本フェローは暗号化技術の第一人者で，世界的権威でもあります．所内の岡本特別研究室の室長として，NTTの牽引役を果たしておられます．

◆晩秋の落ち葉拾い

PF研のある武蔵野研究開発センタは東京都武蔵野市の閑静な住宅街にあります．取材に伺った12月，研究開発センタへと続くイチョウ並木の歩道は，鮮やかな黄色に染まっていました（**写真**）．

敷地内にもさまざまな樹木が植えられています．この時期は，それらの葉が敷地の外に散ってしまうため，11月から12月中旬ごろまで，毎週水曜日の昼休みになると，有志の所員が落ち葉拾いをし，近隣の美化に一役買っているそうです．

今は落ち葉も自分たちで燃やせる時代ではありませんが，思わずヤキイモづくりを想像したのは，筆者だけでしょうか．

写真　イチョウ並木

◆問い合わせ先

NTT情報流通基盤総合研究所
企画部　広報担当
TEL　0422-59-3663
E-mail　islg-pr@lab.ntt.co.jp