安心•安全な暗号システムを目指して：無線LANおよびインターネットで用いられる暗号の安全性評価

神戸大学　大学院工学研究科　教授
森井　昌克

研究の背景

暗号というと小説や映画の世界のもの、あるいは戦争時での指令を秘密裏に送る方法と捉えがちですが、現在では人の生活に密着した見えない空気のように必然的な技術になっています。たとえば携帯電話での通話や課金情報は暗号で守られていますし、鉄道等で利用するICカードも暗号があってこそ、不正に使用されることなく、安心•安全に使えるのです。インターネットを利用して、ショッピングやネット銀行での決済を行う際も、暗号によって不正利用を防いでいます。ネット社会となり、個人でも、その様々な情報をネット上でやり取りする現代、暗号は人々の安心•安全を守る最後の砦なのです。

最後の砦となるべく、その暗号の信頼性自体に問題があってはなりません。本研究では暗号とその暗号の利用方法についての信頼性の評価、特に問題点を指摘し、その改善を与えています。

研究の成果

無線LANでは誰でもその電波を盗聴することができるゆえ、通信内容を暗号化します。その方式としてWEPと呼ばれる事実上の国際標準方式がありました。WEPには数々の問題点がかつてから指摘されていましたが、本研究では最終的に数秒間、暗号化された、すなわちWEPの通信を盗聴するだけで、瞬時に暗号を解析し、解読する方法を提案しました。そして実際にデモを行い、実証致しました。また、逆に、この解読方法を無効にする方法の提案を行い、WEPの改善を提案しています。また、同様に無線LANの暗号化方式として、WPA-TKIPと呼ばれる方式も利用されています。この方式においても、問題点を指摘し、通信内容の解読には至りませんが、暗号通信を妨害する方法を提案しました（図1）。すなわち不正な情報を正しい情報として受け取ってしまう可能性を指摘したのです。次にインターネットでの通信の暗号化に用いるSSL/TLSと呼ばれる方式で、RC4と呼ばれる暗号を用いる場合、その安全性の上で大きな問題があり、個人が解読するのは不可能であるとしても、通信事業者が数多くの通信を傍受することによって、解読出来ることを証明しました（図2）。この結果は政府の暗号評価機関CRYPTRECの推奨暗号リストに評価され、この方式が推奨リストから外されるに至りました。

今後の展望

得られた成果は、多くの人が利用している現状の無線LANおよびSSL/TLSでのデータ暗号化システムを評価するだけでなく、より安全で信頼性の高い方式を導く指針となっています。ストリーム暗号や、それを利用した無線LAN暗号化方式のみならず、これからもますます必要性が高まるネットワーク上での情報保護を目的とした暗号化システム全般、すなわち、個人認証やプライバシー保護をも含む情報制御システムの設計にとって役立つ成果となっているのです。

関連する科研費

平成23-25年度　基盤研究（C）「実装を考慮したストリーム暗号の安全性評価に関する研究」

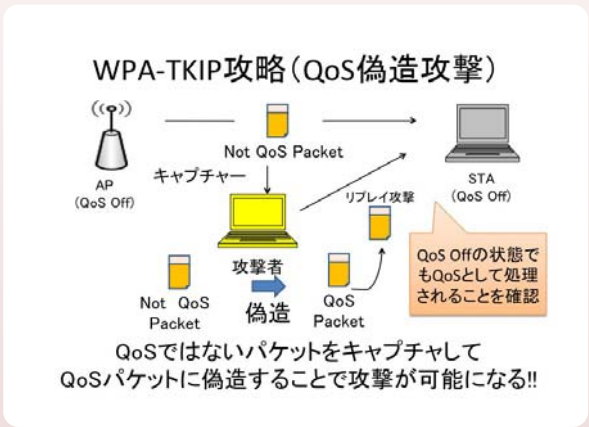

図1　WPA-TKIPに対する攻撃

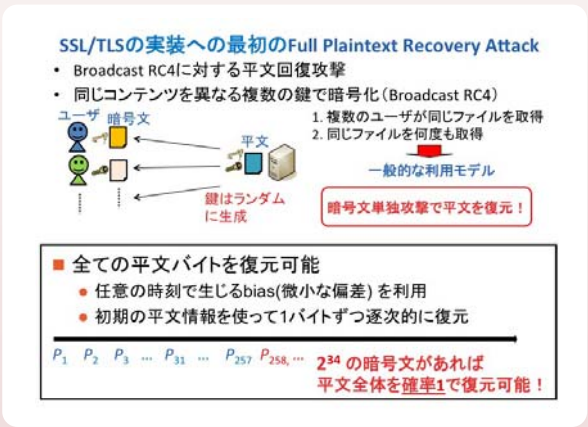

図2　SSL-TLS（RC4）に対する攻撃