暗号プロトコルの安全性評価とポータルサイトの開設

ーICTシステムにおける適切なセキュリティ技術の利用に向けてー

松尾 真一郎（まつお しんいちろう）
ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室 室長

大学院修了後、1996年、NTTデータ通信株式会社に入社、情報セキュリティと暗号の応用に関する研究に従事。
2009年、NICTに入所。2011年から現職。博士（工学）。

ICTシステムのセキュリティを支える暗号プロトコル

我々が日常よく利用する情報システムには、数多くのセキュリティ技術が用いられています。例えば、オンラインバンキングやオンラインショッピングのサイトにアクセスする際には、接続先が正しいWebサーバであることを確認するための認証技術が用いられ、認証が行われた後には通信路上の盗聴に対する安全性を確保するための暗号通信が行われます。また、現在広く普及している無線LANにおいても同じような認証や暗号化が行われています。

これらのセキュリティ技術は、一般的に「暗号プロトコル」と呼ばれます。すなわち、暗号化や電子署名といった基礎的な暗号アルゴリズムとサーバや端末間の通信のやりとりとを組み合わせることによって、認証やプライバシ保護などの、より高度なセキュリティを実現できるようになります。

暗号プロトコルは、前述のようなWebサイトへのアクセスだけではなく、電子メールの認証、データの改ざん防止、タイムスタンプなど幅広い応用に向けた技術が開発されており、ITU、ISO/IEC、IETF、IEEEなどで400以上の技術が標準化されています。

暗号プロトコルの安全性評価とは

このように、暗号プロトコルは我々の日常のネットワーク利用のセキュリティを支えていますが、それぞれの暗号プロトコルが、利用者が期待するセキュリティを確保してくれるのかどうかは大きな問題です。前述のように数多くの技術標準がありますが、一方で暗号プロトコルの脆弱性が報告されることもあります。これは、仮に基礎的な暗号アルゴリズムが安全であったとしても通信との組み合わせの部分の設計が不十分で、そこに脆弱性が発生する可能性があるからです。このような理由から、利用者が期待するセキュリティ要件に合わせて、改めて暗号プロトコルとしての安全性を評価する必要があります。

暗号プロトコルの安全性評価にはいくつかの手法がありますが、基本的な考え方はシンプルで、暗号プロトコルに対して攻撃者が持てる能力を自由に組み合わせて攻撃を行い、プロトコルに期待されるセキュリティを破る行動の組み合わせ（＝攻撃手法）が存在するかどうかをチェックします。このチェックの手法として、状態遷移をしらみつぶしに探査する方法や、論理的に攻撃の発生の可能性を証明する手法などがあります（図1）。

NICTのこれまでの取り組み

NICTでは、これまでに、通信相手が正しい利用者やサーバであることを認証するエンティティ認証プロトコルの国際標準であるISO/IEC 9798-2,3,4に対して、プロトコルの安全性評価を行い、設計上の不備を発見しました。そして、この評価結果と発見した設計上の不備の修正をISO/IECに

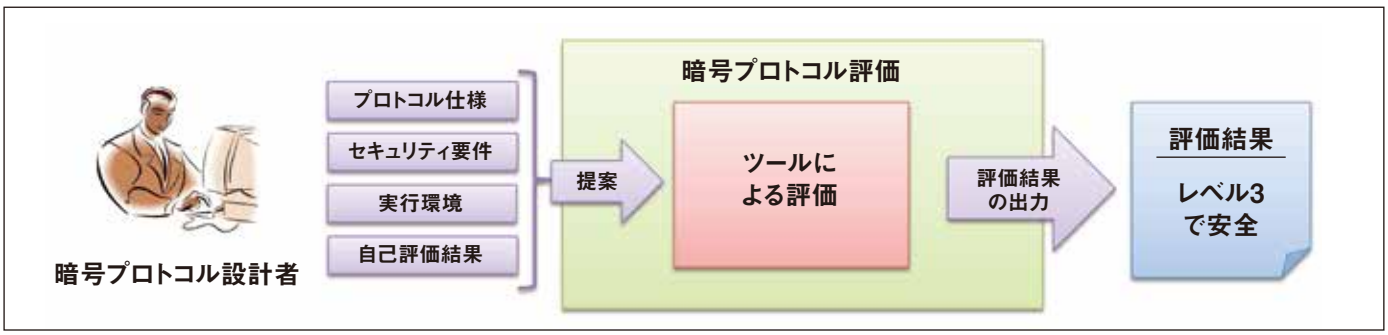

図1　暗号プロトコル評価の基本的な構成

プロトコル保証レベル	PAL1	PAL2	PAL3	PAL4
プロトコル仕様	PPS_SEMIFORMAL プロトコル仕様を準形式的に記述	PPS_FORMAL プロトコル仕様を形式的に記述	PPS_MECHANIZED プロトコル仕様を形式的に記述。その記述はツールに対応した言語で記述され、その言語の文法は数学的に定義されている。	
攻撃者モデル	PAM_INFORMAL 攻撃者モデルを非形式的に記述	PAM_FORMAL 攻撃者モデルを形式的に記述	PAM_MECHANIZED 攻撃者モデルを形式的に記述。その記述はツールに対応した言語で記述され、その言語の文法は数学的に定義されている。	
セキュリティ要件	PSP_INFORMAL セキュリティ要件を非形式的に記述	PSP_FORMAL セキュリティ要件を形式的に記述	PSP_MECHANIZED セキュリティ要件を形式的に記述。その記述はツールに対応した言語で記述され、その言語の文法は数学的に定義されている。	
評価のレベル	PEV_ARGUMENT 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事を非形式的に評価	PEV_HANDPROVEN 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事を、人間の手で数学的形式を整え証明し評価	PEV_BOUNDED 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事をツールを利用した有限チェックで評価	PEV_UNBOUNDED 攻撃者モデルにおいて、対象となるプロトコルがセキュリティ要件を満たしている事をツールを利用した無限チェックで評価

図2　ISO/IEC 29128によるプロトコル保証レベル（Protocol Assurance Level）

対して報告するとともに、NICTの研究者が中心となって同国際標準の修正を行いました。また、この評価結果は、2013年に改定された電子政府推奨暗号リストの「エンティティ認証」の選定にも貢献しています。

暗号プロトコル評価には、様々な評価手法がありますが、評価手法によって評価のきめ細かさが異なります。そこで、評価手法ごとに実現可能な評価レベルを4段階で規定したISO/IEC 29128（Verification of Cryptographic Protocols）を筆者が中心となって策定しました（図2）。

このほか、タイムスタンププロトコル（ISO/IEC 18014）、RFID向けのプライバシ保護認証プロトコルの安全性評価を行い、研究成果として発表しています。

暗号プロトコル評価ポータルサイトの開設と役割

暗号プロトコルの安全性評価結果は、攻撃される可能性がある暗号プロトコルが誤って利用されることのないよう、可能な限り公開される必要があります。特にICTシステムの設計、構築、運用者は、攻撃の可能性がより少ない暗号プロトコルを選択することが重要であり、最新の情報が提供される必要があります。しかし、世界的に見ても、暗号プロトコルの安全性評価結果を集約して、公開する取り組みはありませんでした。

そこで、NICTでは2013年7月1日に、世界初の試みとして、暗号評価プロトコルポータルサイトを開設しました（http://crypto-protocol.nict.go.jp）（図3）。このポータルサイトは、NICTが実施した暗号プロトコルの評価結果を公開しています。掲載されている内容は、一般的に利用可能な暗号プロトコル評価ツールを用いた評価結果であり、

-暗号プロトコルの記述
-求められるセキュリティ機能の記述
-攻撃環境の記述
-暗号プロトコル評価ツールの出力とその説明

がファイルとして提供されています。攻撃の可能性がなければ何も出力されず、攻撃の可能性があればその手順が出力されます。つまり、このファイルを見ることで、個々の暗号プロトコルに対して、攻撃の手順が存在するかどうかを確認することができます。このサイトの掲載内容は、ツールを利用することで誰でも追試することが可能です。

今後の展望

NICTでは、今後も技術標準となっている暗号プロトコルの評価を継続的に実施し、順次評価結果をポータルサイトに掲載していきます。さらに今秋を目処に、国内外の研究者がこの分野の研究を推進する共通基盤となる機能を追加します。その後も暗号プロトコル評価技術を高度化する研究開発の推進や、暗号プロトコル評価の実施と評価結果の提供、国際標準化への寄与などを行うことで、同分野の国際的な中心拠点となることを目指します。

図3　暗号プロトコル評価ポータルサイト