7-8　情報理論的安全性に基づくセキュリティ技術

早稲田篤志　野島　良

安全性の根拠を情報理論に置くセキュリティ技術は、計算機性能の発達による安全性の劣化が起きないという利点があるため注目されている。本稿ではセキュリティ基盤研究室が内外の研究者と協力して開発してきた情報理論的安全性に基づくセキュリティ技術として量子状態を利用した認証方式や、秘密分散法にパスワード認証による復元権限の確認を行うパスワード認証機能付き秘密分散法を紹介する。

1　まえがき

現代暗号技術の多くは、コンピュータを使用しても解くことが困難であるという計算量的安全性をその安全性の根拠にしている。しかしながら、一度安全とされた問題を根拠とした暗号システムであっても、コンピュータ能力の強化や並列性の進化、解法の高度化により、その安全性が危ぶまれるということが起こり得る。この問題に対しては新たな暗号システムの構築や、安全性の根拠となる問題の規模の巨大化により対応されてきている。しかし、問題の規模が巨大化することで、安全性を担保するための計算コストやメモリコストも巨大化することを無視することはできず、また、暗号技術の入れ替えに伴うシステムの更新はサービスの継続性（BCP）に大きな影響を与えるだけでなく、新旧システムの同時運用や旧データとの互換性維持などに伴う安全性低下の懸念も大きい。これに対する方法のひとつとして、情報理論的に安全性を担保する方式が存在する。情報理論的に安全性を担保する方式では計算機の性能や並列性のみならず、新たなタイプのコンピュータ、例えば量子コンピュータの実現等にも安全性が揺るがないセキュリティプロトコルを構築することが可能であるという利点が存在する。このような情報理論的な安全性を有するセキュリティプロトコルの代表的なものとして、量子鍵配送 [1] に代表されるような量子状態を利用した量子セキュリティプロトコル [2][3] や、秘密情報を複数の分散情報に分散保存し、特定の分散情報を組み合わせたときのみ秘密情報を復元でき、それ以外のときには秘密に関する情報を漏らさない秘密分散法 [4] などが挙げられる。

セキュリティ基盤研究室ではこのような情報理論的安全性に基づくセキュリティ技術の研究開発を行ってきた。具体的には、量子状態を利用した認証方式である量子複数同時認証方式の提案 [5] や、特殊な機能を有した秘密分散法である、秘密情報の復元権限を有するか否かをパスワードの所持より認証するパスワード認証機能付き秘密分散法の提案 [6] などがある。また、上記の研究を行うために、内外の研究者の協力を仰ぎ、一定の成果を上げてきた。その連携先としては、NICT 内部においては量子 ICT 研究室の藤原幹生主任研究員をリーダとしたプロジェクトを通じて、量子 ICT 研究室、ナノ ICT 研究室、宇宙通信システム研究室（それぞれ室名等は当時）、パスワード認証機能付き秘密分散法においては、理論面で東京工業大学の尾形わかは教授、実装面で量子 ICT 研究室と協力して研究を行った。さらに、電気通信大学の小林欣吾名誉教授や韓太舜名誉教授から情報理論の理論面でのご指導や、情報理論における技術をセキュリティプロトコルへの応用する際にご助言を頂いた（図 1）。

本稿ではセキュリティ基盤研究室における情報理論的安全性にも基づくセキュリティ技術の成果の概要について述べ、その後、まとめとする。

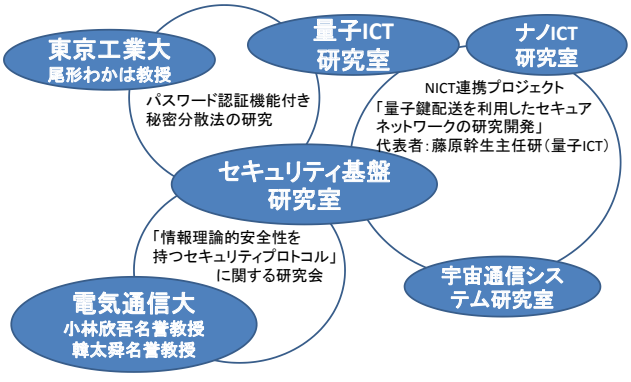

図 1　本研究における内外の研究者との協力体制（名称は当時）

2　研究概要

2.1　量子複数同時認証

2.1.1　概要

本方式は量子状態を利用した認証プロトコルである。通常の認証プロトコルは二者間で実行され、相手が正規のユーザや機器であるかを、一方が他方を、または相互に認証する方式となる。しかし、通常の通信を考えると、送信者と受信者の間には実際には多くの機器（ノード）を介在する。このような複数のノードを経由する通信路において、量子状態を用いて各ノードを一度に認証しようとするのが量子複数同時認証方式である。本研究において、Yang らによる既存方式 [3] では、量子もつれ状態を利用した攻撃を行うとユーザの認証鍵を特定可能であることを示し、この攻撃についても安全な方式を提案した。本成果は電子情報通信学会論文誌にて発表を行った [5]。

2.1.2　提案プロトコル概要と評価

提案プロトコルは n 人のユーザ $A_1, A_2, ..., A_n$ で実行し、ユーザ A_1 が他のユーザを認証する方式である（図 2）。本プロトコルは準備フェイズと認証フェイズからなり、準備フェイズでは信頼できる鍵配布センタが全てのユーザの鍵を生成し、配布する。認証フェイズではユーザ A_1 が作成した量子状態に対して各ユーザが鍵に応じた量子操作を行い、最後にユーザ A_1 が測定を行って、正しい量子状態が測定できたときに他のユーザの認証を受理するという方式である。提案プロトコルでは使用する量子状態と量子操作を工夫することで、通信途中で状態をインターセプトして測定して情報を取得し、その後再送する intercept-resend attack と、攻撃用の量子もつれ状態を送信して、量子操作後に測定することで情報を取得する Fake signal attack with entangled state に対し高い耐性を有することを証明した。特に Fake signal attack with entangled state は Yang らの方式へ適用するとユーザの鍵を確実に暴くこと可能である。Yang らの方式で使用している量子状態と量子操作のペアは Hadamard ゲートを使用した基底変換を用いたものであるため、それを利用したセキュリティプロトコルへの問題提起と、その対策を行った本提案プロトコルの意義は大きいといえる。

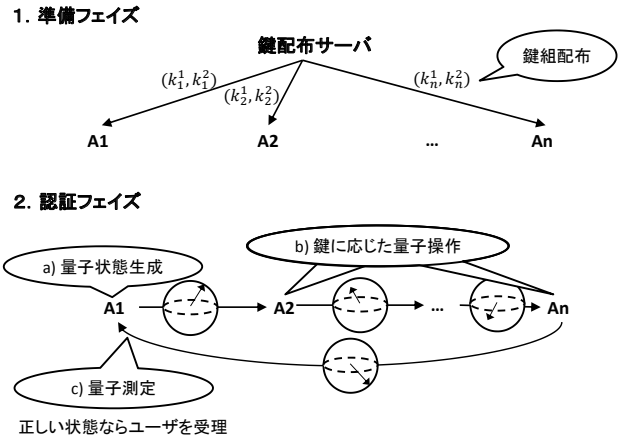

図 2　量子複数同時認証方式概略図

2.2　パスワード認証機能付き秘密分散法

2.2.1　概要

本方式は、秘密分散法にパスワード認証方式を組み合わせたプロトコルである（図 3）。秘密分散法は秘密情報を複数のサーバに分散符号化して保存する方式である。分散符号化された情報はシェアと呼ばれ、ある指定された複数のシェアを集めると元の秘密が復元されるが、1 つでも足りないと秘密に関する情報が、情報理論的に一切洩れない手法である。この秘密分散法のうち最も有名な方法は Shamir により提案された方式 [4] である。Shamir の方式は秘密情報を n 個のシェアに分散し、そのうちの任意の t 個のシェアを集めることで秘密の復元を行える方式であり、(t, n) 閾値秘密分散法と呼ばれる。この秘密分散法に考え得る問題点として、シェアをどのように攻撃者に漏らすことなく各サーバに分散するかといった点や、各サーバはどのように秘密の復元の許可を出すかといった点がある。本研究ではこのうち 2 番目の問題点である各サーバはどのように秘密の復元の許可を出すかという点に着目し、正しいパスワードを知る者のみが正しい秘密を復元できる手法として、パスワード認証機能付き秘密分散法を提案した。同様の手法は Bagherzandi ら [7] や Camenish ら [8] が提案しているが、これらの方式は準同型暗号を利用した結果、全体の安全性が情報理論的安全性から計算量的安全性に落ちてしまっているという点で問題がある。

本研究で提案しているパスワード認証機能付き秘密分散法は、情報理論的安全性を保持した初めての方式である。本研究を遂行するにあたり、東京工業大学の尾形わかは教授にご協力いただき、暗号と情報セキュリティシンポジウム（SCIS）2014 にて発表を行った [6]。また、先にあげた秘密分散法の問題点のうちのひとつめである各サーバにシェアをどのように安全に預けるかという点では、同じく無条件安全性を実現している量子暗号を用いて実現を図るため、量子 ICT 研究室と協力して実装を図っている。

2.2.2　提案プロトコル概要と評価

ユーザは秘密情報 $d \in D$ とパスワード $p \in P$ を持ち、これらを n 台のサーバにシェアとして保存する。秘密情報復元時にはユーザはパスワード $p' \in P$ を入力とし

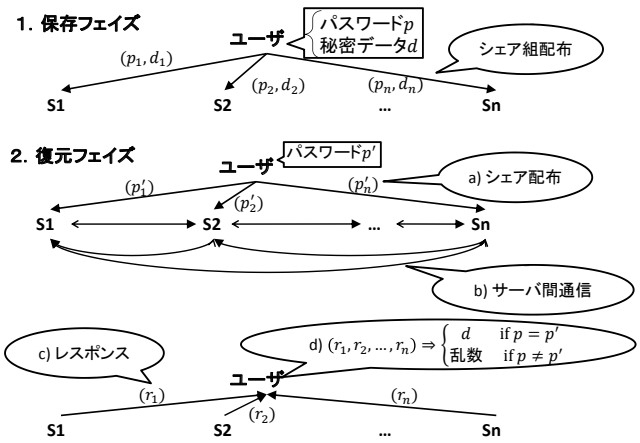

図３　パスワード認証機能付き秘密分散法概略図

て任意の k 台のサーバに保存されているシェアを使って復元を行う。提案プロトコルは保存フェイズと復元フェイズからなり、保存フェイズでは Shamir の秘密分散法を用いて秘密情報 d とパスワード p を保存し、復元フェイズではユーザはパスワード p' のシェアをサーバに送信し、各サーバは保存されている秘密情報のシェアとパスワードのシェアに組み合わせて復元を行うための情報を作成し、ユーザに送り返す。ユーザは送り返された情報を用いて復元を行う。もし $p' = p$ であれば正しい秘密を復元できるが、$p' \neq p$ であるならば乱数が復元され、秘密について情報が得られない方式である。この方式により、本来権限がないユーザにより秘密情報を復元されるということを防ぐことができる。この結果は安全なストレージシステムの作成等の実現に向けた端緒となり、意義は大きいといえる。

3　まとめ

セキュリティ基盤研究室が行ってきた情報理論的安全性に基づくセキュリティ技術に関する研究として量子状態を利用した量子複数同時認証方式と、パスワード認証法と秘密分散法を有機的に組み合わせたパスワード認証機能付き秘密分散法を紹介した。情報理論はセキュリティに限らず重要な概念である。セキュリティ基盤研究室ではこれからもセキュリティプロトコルの開発のみならず、プライバシー保護プロトコルに対して情報理論に基づいた解析を行うなどの研究を行っていきたいと考えている。

【参考文献】

1　C.H.Bennett and G. Brassard, “Quantum cryptography: Publickey distribution and coin tossing,” Proc.IEEE International Conference on Computer, Systems and Signal Processingp. 175, IEEE Press, Bangalore, India, New York, 1984.
2　M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” Phys. Rev. A, vol.159, no.3, pp.1829–1834, 1999.
3　Y. Yang, Q. Wen, and X. Zhang, “Multi-party simultaneous quantum identity authentication with secret sharing,” Science in China Series G: Physics Mechanics and Astronomy, 51, pp.321–327. 2008.
4　A. Shamir, “How to Share a Secret,” Communications of the ACM, vol.22, no.11, pp.612–613, 1979.
5　A. Waseda, “Multiparty simultaneous quantum identity authentication secure against fake signal attacks,” IEICE TRANS. on Fundamentals of Electronics, Communications and Computer Sciences, vol.E96-A, no.1, pp.166–170, 2013.
6　早稲田 篤志，尾形 わかは，野島 良，盛合 志帆，“Active な攻撃者に対して情報理論的秘匿性を持つパスワード認証機能付き秘密分散法 ,” 暗号と情報セキュリティシンポジウム 2014.
7　A. Bagherzandi, S. Jarecki, N. Saxena, and Y. Lu, “Password-protected secret sharing,” In Proceedings of the 18th ACM conference on Computer and communications security, pp.433–444, 2011.
8　J. Camenisch, A. Lysyanskaya, and G. Neven, “Practical yet universally composable two-server password-authenticated secret sharing,” In Proceedings of the 19th ACM conference on Computer and communications security, pp.525–536, 2012.

早稲田篤志　（わせだ　あつし）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（情報科学）
情報セキュリティ

野島　良　（のじま　りょう）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、暗号プロトコル、情報セキュリティ、プライバシー、セキュリティ