平成 23 年 9 月 12 日

資料

玉川大学　量子情報科学研究所

「秘密分散型クラウドの弱点解消に向け
インテリジェント量子暗号の試験可能に」

クラウド・コンピューテイング・システムの安全性に対する疑念は以前より世界中で議論されている。日本では 2 年前より、数理暗号学の成果として知られる秘密分散法を応用するクラウド・コンピューテイング・システムの安全性保証が脚光を浴び、数社によって導入が始まっており、本格的なサービスの普及が進められている。しかし、アメリカでは、秘密分散法の導入に関して消極的である。その理由は以下のような問題点があることによる。

秘密分散法とは、複数のデータセンターに情報を拡散して保存し、一つのデータセンターの情報が盗まれても、そこから利用者の情報を復元できないようにでき、かつ、幾つかのデータセンターが壊れても、残りのデータセンターのデータから全ての情報を復元することが可能となる技術である。以上から、クラウド・コンピューテイング・システムには極めて魅力的な技術といえる。しかし、利用者からデータセンターに向けて情報を伝送するとき、その通信回線上にはデータセンターへのアドレスや経路情報が明確に添付されているため、通信回線に流れている信号をタップすれば、秘密分散法は全く機能しない。すなわち、各データセンターに行くべき信号系列を全て入手可能である。日本の企業は、通信回線が安全であるとの前提でサービスを提供しようとしている。しかし、それは全く根拠のない想定である。

上記のような問題を解決するためには、回線自身を保護する暗号技術の導入が必要不可欠である。

【通信回線保護用の暗号技術の動向】

これまでの高速通信回線の安全性を保証するための暗号技術は伝送されるデータのみを秘匿するものであり、ISO 通信レイヤー規格のレイヤー２あるいは３対応と呼ばれている。しかし、これでは上記のように秘密分散法は機能しない。最近、KVH 社とシエナ社は共同でレイヤー１（回線信号）を秘匿する暗号技術を模索し、アメリカが目指すクラウド安全基準に向けた先行開発を進めているとのニュースをリリースしている。

インテリジェント量子暗号は盗聴者の受信信号を受信時の量子雑音によって見えなくすることによるレイヤー１の安全性保証技術であり、計算機などによる数理的解析が不可能で、盗聴装置の物理的複雑性が実現できないほど大きくなる事によって安全性を保証する。原点は 2000 年度の米国国防総省依頼研究(DARPA)Northwestern 大学プロジェクトとの共同研究としてスタートした Y-00 暗号として知られている。その後、玉川大学方式は改ざん耐性などのインテリジェント機能を持つに至った。上記２社の開発と競合するが、安全性や改ざん耐性などの機能面で優位性を持つため、アメリカ標準対応や防衛対応の回線暗号化技術として期待が持てる。　玉川大学では 1～2.5 ギガビット毎秒、500km 暗号通信システムの開発がほぼ完了しており、大学所有の装置による英米の軍用データセンターにおける運用試験提案に向けて準備を進めている。