学校現場における暗号化ソフトウェアの活用とその重要性

独立行政法人情報通信研究機構：高藪　学：takayabu@nict.go.jp＊
独立行政法人情報通信研究機構：梅野　健：umeno@nict.go.jp
独立行政法人情報通信研究機構：鈴木 紀一：n996224@u-gakugei.ac.jp
東　京　学　芸　大　学：田川 貴章：b032108y@u-gakugei.ac.jp
独立行政法人情報通信研究機構：澤谷 拓郎：b042103f@u-gakugei.ac.jp

1. はじめに　～本報告で取り扱う問題

本報告では，昨今の学校における情報環境の充実にともなって，以前と比較してますます関心が高まっている「セキュリティ」の問題について，暗号技術を利用した解決方法を提案することを目的としている。

特に昨年来，コンピュータネットワークという「バーチャルな」社会においては，例えば「Winny」のような情報共有(Peer-to-Peer)ソフトウェアの機能に起因した情報の漏洩・流失という事件・事故が多発し，個々人の情報をいかにして安全に管理するか，といったことが重要視されてきている。また一方で「現実の」社会においても，ここ最近では，子どもが被害者となる犯罪や事件の数が増えていることから，「子どもの安全」をどのように確保するかということは，重要な課題となっている。

このような社会状況を踏まえて，本報告では「学校」という場において取り扱われる様々な「情報」に注目して，それらの安全性がより確保されるための技術として「暗号」を活用し，加えて，情報教育という観点から「暗号技術」をひとつの授業テーマとして，子どもたちに理解してもらうための方法についても検討したい。

2. 学校における暗号理論の教育

今回の報告では，前節で述べたような問題意識から，「学校」と「暗号」という二者の関連性を考えていく上での第一歩として，学校における情報教育の中で，暗号といったものについて授業の中でどのように触れていくかについて考えることにしたい。特に，本報告では，小学校・中学校・高等学校といった様々な段階の児童・生徒に対して，彼ら／彼女らのもつ知識や理解力に応じて，「暗号」の仕組みやその活用方法を，どのように指導していくかについての検討を行う。そこで本稿では，そのための準備段階として，学校の教育現場において「暗号」について取り上げるにあたって，授業等で触れなければならないであろうと思われるトピックスについて整理を行っていく。

「暗号」について学習するにあたって，最も基本的な，かつ最も重要な事柄は，「暗号アルゴリズム」と「鍵」についての理解であるといえるだろう。これらの概念は，暗号理論を理解するにあたっては，お互いに不可分なものである。例えば，「暗号アルゴリズム」について十分に理解できていたとしても，「鍵」についての理解が不十分であれば，暗号を利用することはできないし，その逆もまた同様である。すなわち，様々な「暗号アルゴリズム」や「鍵」が存在する中で，それぞれのアルゴ

リズムとそのアルゴリズムに対応する鍵をどのように使い分けていくか，といったことについて児童・生徒に教える必要があるというわけである。さらには，このことと関連して，現在の暗号技術の中心である「公開鍵暗号」に関して，それがどのような発想に基づくものであるのか，ということについても理解する必要があるといえるだろう。

以上のことを前提として，本報告では，実際の指導内容の例についてより具体的に提案していくことにしたい。

3. 学校における暗号ソフトウェアの利用

前節までの議論を踏まえて，ただ暗号の理論について授業でどのように扱っていくか，ということのみならず，本報告ではさらに一歩進んで，現実の学校での様々な場面において，実際に「暗号化ソフトウェア」をどのように活用することができるかについても議論を行っていく。この場合に特に重要な観点として，「誰が暗号化ソフトウェアを利用するか」という点がある。そのことに関して，本報告では，主に次の二者について考察を行う。

一つは，学校において教職員が業務で使用するコンピュータについて，その情報の安全性を確保するために「暗号化ソフトウェア」を利用するという提案である。第 1 節でも述べたように昨今の個人情報の流出や漏洩といった事件から，学校の内部(児童・生徒，およびその保護者など)だけではなく，その外部からも，学校での情報の取り扱われ方について大きな関心が集まっている。そのことから，学校内部の情報をどのようにすれば安全に取り扱うことができるかについて，本報告では具体的な事例を挙げて紹介することにしたい。

もう一つには，児童・生徒が学校においてコンピュータを使用する際に，「暗号化ソフトウェア」がどのように利用可能であるかという点である。このことは，当然のことながら，前節で述べた暗号理論についての教育を行う場面でも大きな役割を果たすが，それ以上の教育効果も期待できる。なぜならば，実際に「暗号化ソフトウェア」を使用することは，子ども達にとっては「守るべき情報とは何であるか」「どのような情報を公開するのか」といった情報リテラシーについて学ぶことにつながるからである。

以上の二つの観点から，学校における「暗号化ソフトウェア」の利用というテーマで，その具体的な方法について，本報告では提案を行っていくことにしたい。

4. まとめ　～報告にむけて

今回の「2006 PC Conference」では，前節までに述べた「学校での暗号理論の教育」と「学校での暗号化ソフトウェアの利用」について，ポスターセッションによって，より具体的な事例の提案を行う。そのことに加えて，実際の「暗号化ソフトウェア」のデモンストレーションもあわせて行う予定である。なお，デモンストレーションの際には，本報告の目的に合致する「CIPHERON™」シリーズ(株式会社カオスウェア[1])製)を使用する。

5. 参考文献(抜粋)

○ フレッド・パイパー／ショーン・マーフィー(著)，太田和夫／國廣昇(訳)，『1 冊でわかる 暗号理論』，岩波書店，2004 年

○ 結城浩(著)，『暗号技術入門 —秘密の国のアリス』，ソフトバンククリエイティブ，2003 年

[1] http://www.choasware.com/