情報システム工学科　平成１４年度後期「自主課題研究」

研究テーマ：電子署名の安全性について

名列番号０１６　狩野　孝太
名列番号０６７　安本　庸逸（共同研究者）

1.　まえがき

インターネットが普及した昨今、見知らぬの他人と気軽に**電子商取引が当たり前のように行われている。しかし、電子上の取引は筆跡なども残らない事も多く、相手方の完全性及び何か起こった際の記録を確認する必要性がある。**

今回は電子上で一般的に使われている電子署名を簡略したものを作成し、それに対する安全性などについて考察してみた。

2.　研究課題

ハッシュ関数生成プログラムである「SHA-1」を作成し、それについての理論的・実際の動作についての考察を行う。

また、電子署名に対する基本的理解を深める。

3.　研究方法

１、プログラムの作成

２、インターネット・書籍での研究

「SHA-1」とは、電子政府推奨暗号リストに名を連ねている電子署名の一部分であるハッシュ値 120 ビットを出力するプログラムである。本来、新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、そちらの方が望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

また、プログラムの作成の都合上、あまり大きいサイズのものは作成に手間が掛かり、それだけで実験が終わってしまったり、出力結果が複雑すぎたりして、データの検証が行えない可能性があったので、その点を考慮している今回は SHA-1 を扱っている。

4.　実験結果と考察

「SHA-1」の安全性については、実行時間計算不可能であるということが確認できた。

5.　まとめと今後の課題

電子署名の安全性は確認できたが、日々、進化していく計算機の計算量に耐えうる暗号は無く、どんな暗号も時間をかければ必ず解けてしまうという事がわかった。

そういった事態を回避するためにも、もっと複雑なアルゴリズムや、生態認識のような情報量の多い暗号を考えたり、暗証番号を厳重に保護したり、こまめに変えたりするなど、自分の防衛意識を高めることも重要だと感じた。

6.　参考文献

『暗号技術入門 ―― 秘密の国のアリス』結城浩