情報システム工学科　平成１７年度後期「自主課題研究」

研究テーマ：電子署名の安全性

名列番号０６７　安本　庸逸

１．まえがき

現在、インターネットにおける取引が頻繁に行われていますが、**見ず知らずの人を相手に電子商取引などが行われるという特徴があり、「紙」ベースのように筆跡なども残らないから、相手方の本人性を確認する必要性があります。そのために、**一般的に使われているものとして、電子署名があります。

２．**研究課題**

電子署名について調べてみようと思いました。また、具体的に理解するために、実際に電子署名を作ることができるプログラムを作ってみようと考えました。

実際に電子署名ついて調べてみると、暗号技術についても知らなければならないということがわかったので、それについても並行して調べていくこととしました。

ただ、調べていくうちに、電子署名は安全なのか？という疑問がでてきました。そのため、それについても、調査、考察していくことにします。

３．研究方法

それぞれ、インターネットや、文献を調査し、実際にプログラムを製作し、試しました。

製作プログラム

ハッシュ関数

RSA暗号化復号化

電子署名

以上を作り、実際に動作させてみました。

４．考察、まとめ

電子署名は今のところ、安全である、という結論でかまわないと思いました。ただし、きちんとした信用できる認証機関で証明を受けることが条件になります。

しかし、今、安全だとしているが、技術が進歩すれば、今までの暗号法が解読されてしまったり、ハッシュ関数などは、解読のかなりの指針が出てしまって、次世代のハッシュ値が求められてきてしまっています。便利になるために、技術が進歩するのはうれしいですが、その進歩によっても、安全を失う可能性もあるのでも、イタチごっこのようで大変だと感じてしました

５．反省、今後の課題

反省点としては、なかなか検証ができず、数値を見ても、あまり、新しい発見ができなかったことです。また、どのように検証するかや、自分の個性を出す、というのが難しく、きちんとできた自信がないです。

課題は、もっとべつの公開鍵暗号方式でも試したりしたかったですが、技術と時間の不足でした。また、SHA-1 の有効なアタック方法を具体的に調べようとしましたが、完全版の論文が見つからなかったり、英語で書かれているのを翻訳した為か、うまく理解できなかったのは、残念でした。実際に、解けたとしても２の６９乗では、計算させるのは、無理だっただろうなと思うとこれもまた、残念です。

６．参考資料

ブルース・シュナイアー (著), 山形 浩生 (訳)
暗号技術大全　　他多数