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：住基ネットと暗号

名列番号　０４５　　寺下　知宏

１、まえがき

現在の IT 社会で暗号はいろいろなところで使われて、実用化されている。その中でも、住民基本台帳ネットワーク（住基ネット）において暗号がどのように使われているかを研究することにした。

２、研究課題

住基ネットがどのようなものか調べる。住基ネットにおけるデータ通信と住基カードにおいて暗号がどのように使われているかを調べる。

３、研究方法

基本的にはインターネットによって情報を得ることにした。さらに実際に市役所に行って、住基カードを入手し、それについても調べた。

４、考察

住基ネットとは、住民の居住関係の公証、選挙人名簿の登録などの住民に関する事務の処理の基礎となる制度である。住民１人１人に１１桁の住民票コードをつけ、それを基に迅速な事務処理を行うため、各市町村や県のネットワーク化が進んだ。

まず、データの通信について考えた。データを暗号化するときには、公開鍵暗号方式と共通鍵暗号方式の２つを用いて行っていた。しかし、どの暗号方式が使われているかは秘密事項となっていたので自分で考えてみることにした。最高度の安全性が必要であると考え、その結果、公開鍵暗号は RSA－PSS、共通鍵暗号は AES を用いていると考えた。

次に、住基カードについて考えた。これは住基ネットのサービスの１つで希望した住民に発行される。このカードには、ESIGN、RSA、楕円曲線暗号が対応していることが分かった。さらに、耐タンパー性によってスキャニングなどから情報が流出するのを防いでいることが分かった。

５、まとめ

住基ネットという個人情報を扱うシステムにおいて、そのデータを第三者から守るために様々な工夫がされて暗号が用いられていることが分かった。

しかし、暗号の解読方法は日々進化しているのでより発展させて、住民が安心できるようなシステムにしてほしいと考える。

６、参考文献

http://www.soumu.go.jp/c-gyousei/daityo/　他