デジタル署名と公開鍵基盤の研究

情報システム工学科　　０１２　　片山　裕貴

１　公開鍵基盤(ＰＫＩ)とは

PKIは広範囲に効率的に公開鍵暗号技術とデジタル署名技術を使用できるようにし、認証局サービスと直接関係付けるもの、金沢大学で使われているVPNもその一種。

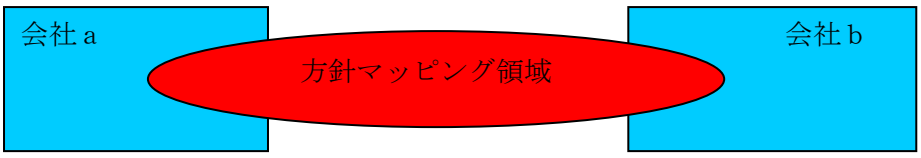
２　研究内容

書物、インターネットなどを使いデジタル署名と公開鍵基盤についての理解を深める。その後、自分で公開鍵基盤を考え、設計してみる。

３　考察

海外企業との業務提携、地域の医療ネットワークなどを想定して、実際にＰＫＩを考え、設計した、その際にはインターネットで病院のセキュリティシステムなどについても調べた。また金融機関のATMシステムについても調べた。まだあまり使われていない、クロス認証という相互認証システムが使われていた。クロス認証はまだ改良、研究の余地が多いが技術が確立すればセキュリティシステムが大きく発展すると考えられる。

クロス認証の例　赤い領域で会社ａと会社ｂの情報が共有される。改良が簡単で等価な関係で共有できるのが利点。



４　感想

実際に考えてみてセキュリティ面以上に実際にどのようなものが求められているかを調べることや、考えることに苦労した。効率とセキュリティのバランスを考えることが重要だと感じた。無論、全くの新しい技術の開発も重要であるが。

＜参考文献＞　不思議の鍵のアリス
デジタル署名と暗号技術　＜ウォーウィック・フォード　署＞