# CRYPTO98を用いたCAD図面の暗号化と配送方式*

6G−8

向井　将**　　井上幸美**
立命館大学大学院理工学研究科**

## 1. はじめに

CADのデータを公開されたネットワーク上で送受信する際、常に第三者の目にふれる。また、電子的なデータであるため容易にデータが複製される危険性がある。これを防ぐ手段として、データを暗号化し、かつ、署名に相当する検印を施して、CAD図面を配送するシステムを、これまで開発してきた暗号システム“CRYPTO98”上に構築し、その動作特性を調べたので報告する。

## 2. CRYPTO98

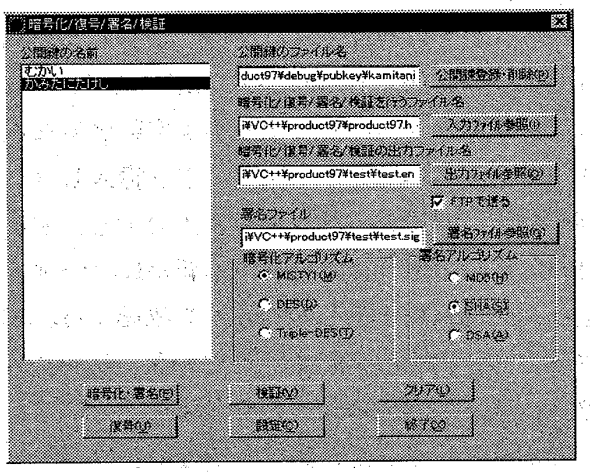


図1　CRYPTO98

CRYPTO98は、三菱電機が開発した暗号ライブラリ“PowerMISTY”を目的に応じて図 1のようなダイアログから自由に組み合わせ、暗号文、ディジタル署名をネットワークを介して送受信する機能をもつアプリケーションシステムで、対称暗号方式(MISTY1[1] 、DES、Triple-DES)、非対称暗号方式(RSA)による暗号化・復号化に加えて、ディジタル署名(MD5、SHA、DSA)の各方式の選択とそれらの方式によって作り出された暗号文・署名の送信機能を有している。

### 2.1. 暗号化・署名

CRYPTO98は、暗号化を行う際に、対称暗号だけで暗号化はせず、同時にディジタル署名を作成する。そして、その署名をRSAにより暗号化し、暗号文、署名を一つの組にして相手に渡す。また、CRYPTO98は、MD5、SHA、DSAのどれかを選択して署名の作成を行うことができる。MD5、SHAを用いてハッシュ値を生成し、それをRSAにて暗号化を行う。

### 2.2. 復号化

CRYPTO98で復号化を行う時は、暗号化の際、ファイルに埋めこんだ暗号化アルゴリズム情報をもとにして復号を行う。また、同時にディジタル署名の検証も行う。

### 2.3. ディジタル署名の検証

CRYPTO98で署名の検証を行う際には、署名ファイルに埋めこまれた署名アルゴリズムの情報をもとにして、平文と署名の間で検証処理を行う。

### 2.4. データの配送

CRYPTO98では、暗号文、ディジタル署名をネットワークを介して送信することができる。データの送受信には、HTTPとFTPを用いる。

データの送受信の流れを、以下に示す。

1. 送信者は、CRYPTO98を用いてデータの暗号化、ディジタル署名の作成をする。
2. 自ドメインのHTTPサーバに1.で作成したファイルをLHAにて圧縮して転送する。
3. 送信者は受信者に向け、HTTPサーバ上のディレクトリ(URL)を電子メールによって伝える。

---

* A method of delivering ciphered CAD files on CRYPTO98, Masaru Mukai, Yukiyoshi Inoue
** Department of Computer Science, Ritsumeikan University.
1-1-1 Nojihigashi, Kusaysu city, Shiga pref., 525-8857, Japan.

4. 受信者は送信者からのメールに示されているURLからデータを入手する。
5. データを入手した受信者は、CRYPTO98を用いて、データの復号、検証を行う。

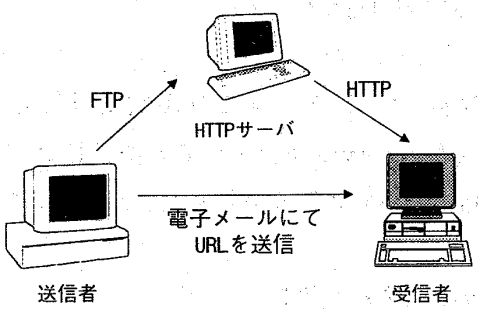


**図2　ファイル送受信**

前述したファイル送受信の流れを図にすると図 2のようになる。一般に、暗号データの送受信には、主に電子メールを用いている例が多いが、メールサーバ間のネットワークに負担をかけ、ネットワーク資源を浪費する [2]。そこで、CRYPTO98 では HTTP、FTP を用いてデータを配送する方式を採用した。

## 3. 検印されたCAD図面の暗号化

CAD ファイルに対する検印のイメージは、従来のCAD 図面に対して行っていた印鑑での“検印”のイメージに近い。今までの“印鑑”の代わりに図3に示すように、片方向関数と公開鍵アルゴリズムで同等のことを行う 。

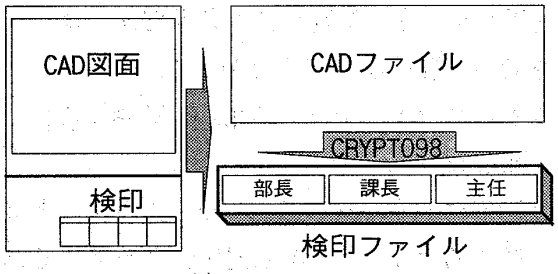


**図3　CRYPTO98による検印のイメージ**

図 4に示したファイルは、dxf 形式の CAD ファイルをレンダリングし、画像データにしたものである。この dxf 形式の CAD ファイルのファイルサイズは、1,122,500bytes(平文時)である。

CRYPTO98 を使用して、図 4に示したファイルに対し暗号化、検印を施すのに要する時間の計測を行った。暗号化処理の際に使用したアルゴリズムには、MISTY1 と Triple-DES を用い、検印の際のアルゴリズムには MD5、SHA を用いた。それらを組み合わせ、暗号化、検印のパターンを 4 種類作成し、またファイルサイズを 1～4 倍まで変え、それぞれの処理に要した時間を計測した。その結果を図 5に示す。

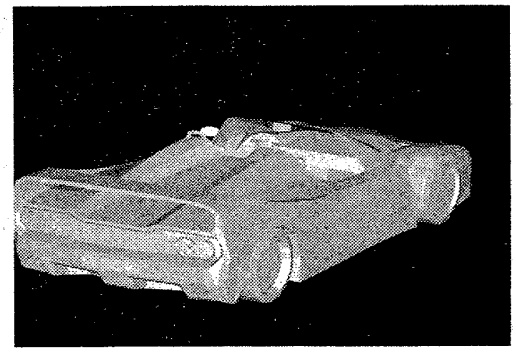

**図4　サンプル CAD ファイル(dxf 形式)**

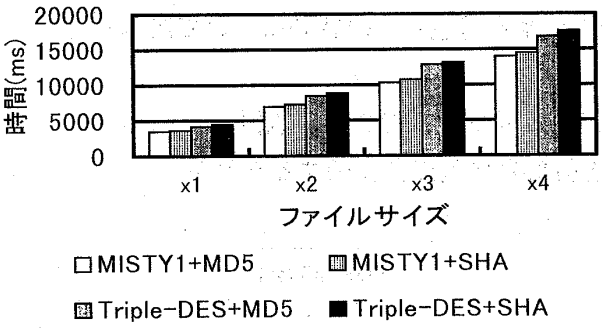


**図5　データサイズと検印に要した時間の関係**

図 5に示したグラフから、CRYPTO98 を使用した暗号化、検印に要する時間は、アルゴリズム、ファイルサイズに関らず 1Mbytes あたり 3 秒～4 秒であり、一定のスループットが得られることがわかる。

## 4. おわりに

本稿では、CRYPTO98 を使用した暗号データの配送方式、そして、CAD ファイルを用いて暗号化・検印の評価について述べた。今後は、HTTP サーバからデータを受信する際に、ユーザ認証を行い、より安全性の高いデータの送受信を実現する予定である。

### 参考文献

[1] 松井充 : ブロック暗号アルゴリズム MISTY, 信学技法 ISEC96-11(1996-07), 電子情報通信学会

[2] S. Hambridge : Netiquette Guidelines, RFC1855(1995)