

サイバー情報セキュリティに関する研究

石 田 裕 生^{*}・牧 野 勝^{**}

Study on Cyber Information Security

Yuusei Ishida and Masaru Makino

The internet commerce has been greatly proceeding and the importance of security technology in the information systems has ever been increasing. In this paper, the authors research security systems against information crimes as well as unlawful access to information resources.

First, we describe security concept and then show functions to construct security systems. Second, the authors introduce cipher technology that plays important role in the information systems. In the cipher technology, we have common key cipher and public key cipher. The authors express example of authentication technology that is one of the most important technology for application of public key cipher.

Finally we introduce Mitsubishi Misty cipher system that is composed of common key based cipher. As application systems in this research, the authors examine method of electronic settlement by using security systems.

1. はじめに

近年インターネットコマースの進展はめざましく、さまざまな技術が開発されている。インターネットコマースを支える技術としては、電子認証、電子決済のような安全性を確保する技術が不可欠であるが、それ以外に既存のシステムとの接続性やシステム規模の変化、多様性に応じて柔軟なシステム構築が可能な拡張性を確保するための技術が必要とされてきている。

このような背景の中、インターネットコマースにおいて、より安全に、より快適に、より拡張性を考慮したセキュリティシステムの検討を進めている。また三菱電機が開発した暗号アルゴリズム「MISTY」を使ったセキュリティシステムもその対象としている。

1.1 サイバー情報セキュリティ

サイバー情報セキュリティは情報システムの機能が、外部から有害な干渉を受けることなく仕様通りに働き、安定して利用可能な状態を保つためにある。サイバー情報システムではデータ破壊や、盗用が予想されるいくつかの局面に対して複数のセキュリティレベルを用意している。米国防総省では 5220.28 規格（通称オレンジブック）でクラス A1、B3、B2、B1、C2、C1、D までの 7 段階のセキュリティレベルを定義しており、D が最低のレベルとなっている。本研究では、盗用やなりすましに対し、暗号化やアクセス制御などに重点をおいてセキュリティシステムの考察を行う。

* 電気工学専攻大学院生（前期課程） ** 経営工学科

2. 暗号技術

本論文で扱う暗号とは次のような定義、すなわち「元のデータ（平文）を送信者と受信者以外の人には解読不可能なデータ（暗号文）に変換する（暗号化）、または元に戻す（復号化）ための技法」に従う。情報セキュリティにおける代表的な暗号方式として利用されている RSA 暗号や Misty 暗号等も上記の暗号の定義に当てはまる。このタイプの暗号は、データを数値列の形で表現して数学的に取り扱うことができる。

2.1 暗号の基本原則

一般的に暗号化と復号化には、平文と暗号文を関連付けるためのアルゴリズムと鍵と呼ばれる秘密の値が必要となり、現在普及しているすべての暗号方式（RSA 暗号や DES 暗号等）では、そのアルゴリズムを知っていても、鍵の値がわからなければその暗号文を解読することは不可能である。

暗号の方式としては、大別して共通鍵暗号方式と公開鍵暗号方式がある。これらの使い分けは暗号化の目的による。以下にこれらの暗号方式の特徴について述べる。

2.1.1 共通鍵暗号方式の問題点

共通鍵暗号では暗号化と復号化を同じ鍵で行う。共通鍵暗号の原理は比較的単純で、基本的には換字と置換を組み合わせたものである。換字とは文字を別の文字に置き換えるものであり、置換とは文字の順序を置き換えるものである。この方式の長所と短所を以下に示す。

長所：ロジックが比較的単純なので、暗号化の計算時間は公開鍵暗号と比べて短くて済む。

短所：送信者と受信者の間で安全に鍵の受け渡しを行うことが困難である。通信相手の数だけ複数の鍵を持たなくてはならない。

2.1.2 公開鍵暗号方式の問題点

公開鍵暗号では暗号化と復号化にそれぞれ一つずつ異なる鍵を必要とする。すなわち 2 種類の鍵が必要となる。各利用者は一対の暗号化用の鍵と復号化用の鍵を生成し、暗号化用の鍵を公開（公開鍵）し、復号化用の鍵を秘密（秘密鍵）にしておく。公開鍵暗号方式の長所と短所を以下に示す。

長所：送信者と受信者の間で安全に鍵の受け渡しを行うことが容易である。

短所：公開鍵暗号方式の原理は共通鍵暗号方式のそれと比べて複雑である。したがって暗号化の計算時間は共通鍵暗号方式と比べて長くなる。

公開鍵と秘密鍵が特別な関係で結ばれ、暗号化と復号化がきちんと機能するための原理を実現するには、整数論を用いた数学的な仕掛けが必要となる。代表的な公開鍵暗号方式としては、RSA 暗号、楕円曲線暗号、エルガマル暗号などがあげられる。いずれも整数論を利用した方式である。RSA 暗号方式の原理は、大きな数の素因数分解が難しいことに基づいており、経験的に安全性が確かめられている。以下に RSA 暗号方式について述べる。

2.1.3 RSA 暗号方式の秘密鍵と公開鍵の作成

RSA 暗号方式では、暗号化を行う前に予め以下の手順に従って秘密鍵と公開鍵を作成しておく。

- (1) 2 つの大きな素数 p 、 q を選択する。
- (2) $n = pq$ と $\phi(n) = (p-1)(q-1)$ を計算する。この n を係数と呼ぶ。
- (3) $\gcd(e, \phi(n)) = 1$ の関係をもつ乱数 e （公開指数）を選択する。ここに \gcd

とは、2つの引数の最大公約数を意味する。この公開指数 e と係数 n が公開鍵 (e, n) となる。

(4) $1 = d e \bmod \phi(n)$ となる d (秘密指数) を計算する。この秘密指数 d が秘密鍵となる。
いま平文を X 、暗号文を Y とすると、 $X < n$ であれば、以下の関係式が必ず成り立つ。

$$X^e \equiv Y \pmod{n} \quad \dots\dots\dots \text{暗号化}$$

$$Y^d \equiv X \pmod{n} \quad \dots\dots\dots \text{復号化}$$

なお、エルガマル暗号方式の原理は離散対数と呼ばれる問題が難しいことに基づいており、楕円曲線暗号方式の原理は、楕円曲線と呼ばれる曲線上の点の間で演算が定義でき、その上で離散対数問題の類似物 (楕円離散対数問題) が作れることに基づいている。

2.2 計算量と安全性

一般に暗号方式の安全性は、復号化に必要な鍵を知らない状態で、暗号文を復号するための鍵を探索するのにかかる計算量 (鍵の長さ) によって決まる。暗号アルゴリズムの中には、可変長の鍵を持っているものがある。このような方式は、鍵の長さを長くすることでより安全にすることができる。鍵の長さを1ビット増やした場合、その鍵を使って正当に暗号化 (復号化) するための計算量はほんの少ししか大きくならないが、不正に解読するための計算量は2倍になる。

2.3 共通鍵を公開鍵暗号方式で送信する

共通鍵を相手に安全に受け渡ししたい場合、共通鍵を相手の公開鍵で暗号化する。相手は自分の秘密鍵で復号化することにより、共通鍵を入手できる。この共通鍵を使用して、送られたメッセージの暗号文を平文に復号化することができる。

3. 認証技術

以上に秘匿機能としての狭義の暗号技術について記述したが、ここでは広義の暗号技術において秘匿機能と対をなす認証技術について述べる。

認証とは、人あるいは物が正しい (偽造されていない) ものかどうかを検証する作業のことである。この認証は暗号技術の中でも最も基本的な技術の一つである。認証技術としては、通信相手の正当性を認証する相手認証やデータの正当性の認証を行うデジタル署名などがある。

3.1 相手認証

ネットワークを経由してパスワードが送られることは一般的であるが、盗聴の危険などを伴うので、安全性において問題がある。そのため、暗号・認証機能を使って安全に相手認証を行うことができる手法が要求される。例えば、以下のような方法が考えられている。

- (a) 使い捨てパスワード認証方式
- (b) 一般パスワード認証法
- (c) ネットワーク層アドレスに基づく認証方式
- (d) 共通鍵暗号に基づく認証方式
- (e) ゼロ知識対話証明を利用した方式

これら以外に、次に述べるデジタル署名を利用した相手認証方式なども有効である。

3.2 デジタル署名

デジタル署名 (電子署名、電子印鑑) は、自己否認を避けてデータ正当性の認証を行うため

の方式である。これは公開鍵暗号方式を利用することによって実現される。デジタル署名は、データの正しい作成者（あるいは送信者）とデータの正当性（データが改ざんされていないこと）を証明するためのもので、本人しか作成できないものでなければならない。しかも、その署名の正当性は誰にでも検証できるものでなければならない。

このようなデジタル署名を実現するためには、公開鍵暗号の原理を利用する。つまり署名文を作成できるのが秘密鍵（署名鍵）を持っているユーザだけであることを利用する。公開鍵（検証鍵）は公開されているので、検証は誰にでもできる。

実際にデジタル署名を利用する場合には、ハッシュ関数と呼ばれる一方向性関数であるデータ圧縮関数を併用する。その方法を簡単に説明すると次の通りになる。

- (1) まず、平文Mをハッシュ関数Hにより基本単位の長さ以下H(M)まで圧縮する。
- (2) デジタル署名するときは、このH(M)に対して秘密鍵で暗号化（署名）し、それを平文Mとともに送る。
- (3) そして、受信者は受け取った平文Mをハッシュ関数Hで圧縮し、それと署名を検証する。

この手法は平文Mが鍵の長さよりも長い場合に使われる。デジタル署名を実現する方式としては、例えば素因数分解に基づく RSA 署名方式や ESIGN 署名やフィアット・シャミア署名、離散対数に基づくエルガマル署名、DSA 署名やシュノア署名、楕円離散対数に基づく楕円エルガマル署名、楕円DSA署名や楕円シュノア署名などがある。

4. PGP と Outlook を用いた認証実験

PGP(Pretty Good Privacy)は電子メールやファイル記憶型アプリケーションで利用できる機密保護と認証のサービスを提供している。また PGP では RSA 公開鍵暗号と MD5(一方向ハッシュ機能)を利用して、受信メッセージ認証を受信者に保証するデジタル署名を作成する。その処理の手順を以下に示す。

- (i) 送信者がメッセージを作成する。
- (ii) MD5 を利用して、そのメッセージの 128 ビット・ハッシュ・コードを生成する。
- (iii) 送信者の秘密鍵を使用してハッシュ・コードを RSA に暗号化し、それをメッセージの前に付加する。
- (iv) 受信者は RSA と送信者の公開鍵を使用してハッシュ・コードを解読し、復号化する。
- (v) 受信者はメッセージのハッシュ・コードを生成し、解読したハッシュ・コードと比較する。
このコードが一致すると、メッセージの正当性が認証される。

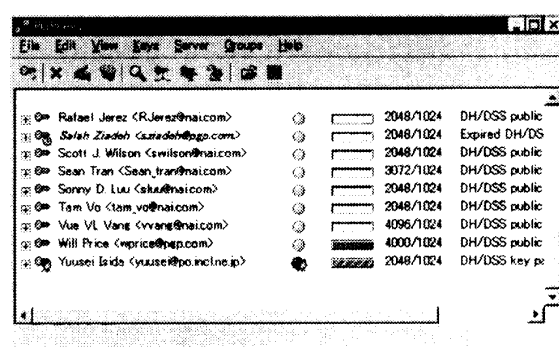


図1 PGP の公開鍵(ユーザ対応)

次に Outlook は S/MIME を利用して暗号とデジタル署名を行う。S/MIME では送信すべき平文に対し何らかの暗号処理を施し、さらに電子メールの規約に沿う形にし、暗号化されたメッセージを作り上げる。その処理の手順を以下に示す。また、暗号方式として公開鍵暗号では RSA を使い、共通鍵暗号では DES、Triple-DES、RC2が推奨されている。メッセージダイジェスト(ハッシュ関数によるデータ圧縮)では

MD-5、SHA-1 が使われている。

- (i) 送信者がメッセージを作成し、電子署名を付け、メッセージを共通鍵で暗号化する。
- (ii) 共通鍵を公開鍵で暗号化する。
- (iii) MIME 処理するがこのときメッセージはバイナリ方式のため 8 ビットであり、Base64 でエンコーディングし、7 ビットに変換する。
- (iv) MIME 処理をし、署名が「smime.p7m」というファイルとなり添付される。
- (v) 受信者は S/MIME に対応したメールと受信者の個人鍵により、復号化し、認証する。

PGP と S/MIME の大きな違いは認証局 (例 VeriSign) を利用するかどうかの違いである。S/MIME では認証局が各自の公開鍵を証明書という形で保証するのに対し、PGP ではユーザ同士が鍵を配布するサーバーなどで鍵を交換し、相互に信頼関係の確立を行わなければならない。またフリーウェアの PGP では規制などの理由から商用で使うには問題が多いが、S/MIME では商用で使うには何ら問題はない。

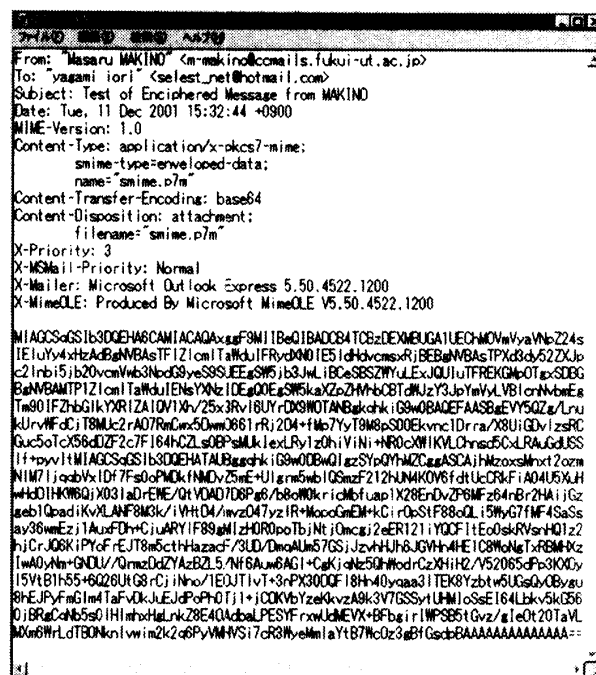


図 2. 暗号化された署名付メッセージ

5. Misty の特長

暗号アルゴリズム MISTY は三菱電機が開発した共通鍵型の暗号方式のことで、データを 64 ビットのブロックに区切って暗号化する。鍵の長さは 128 ビット。DES などと同じように暗号化と復号化に同じプログラムが用いられ、共通鍵暗号の多くを効率良く解読してしまう線形解読法や差分解読法に対しても十分な強度を持つように設計されている。MISTY は強度と速度を向上させるため、構造上の新しい工夫をしている。その結果、以下のことが実現されている。

- (a) 汎用的な暗号解読法である、差分解読法と線形解読法に対する安全性を定量的に評価することができる。
- (b) 暗号化速度と暗号強度の関係を明示することができるため、ユーザのセキュリティニーズに応じた暗号の利用が可能である。
- (c) 並列処理が可能なアルゴリズムなため、I C カードから高性能ワークステーションまで、あらゆるプラットフォームで高速性を実現し、ソフトウェアだけでなくハードウェアでも十分な高速化が可能な構造を設計することができる。

6. セキュリティシステムの構造

セキュリティシステムは図 3 に示すようにアプリケーションレイヤー、ミドルレイヤー、ベースレイヤーの 3 層から成り立つ。

(1) application レイヤー

application レイヤーでは以下の機能があげられる。

- (a) メッセージ暗号化
- (b) アクセス制御
- (c) デジタルコンテンツ配布
- (d) デジタル認証書発行と管理
- (e) ファイル暗号化

(2) middle レイヤー

middle レイヤーでは分散オブジェクトを中心にし、暗号化ソフト、VPN、管理・監査ソフト、ネットワーク、データベースなどを用いてシステムを構築する。

(3) base レイヤー

base レイヤーでは、その中心はプラットフォーム (OS) である。各層にはファイアーウォールを設けて、安全性を高めている。

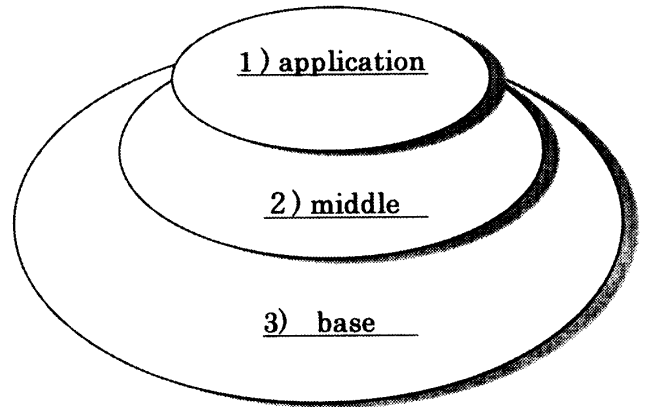


図3 セキュリティシステムの構造

7. 秘密重要情報ファイルの暗号化分析実験

Microsoft 社の暗号化ファイルシステム (EFS:Encrypting File System) は公開鍵暗号をベースにしており、CryptoAPI アーキテクチャを利用する。各ファイルはユーザの秘密鍵・公開鍵のペアとは関係なく、ランダムに生成された鍵を使い暗号化される。EFS は暗号アルゴリズムとして DES (Data Encryption Standard) を使う。また、EFS はリモートのファイルサーバに保存されたファイルの暗号化と復号化もサポートしている。エクスプローラを使ったファイル暗号化手順を以下に示す。

- (i) エクスプローラを起動する。
 - (ii) フォルダやファイルの名前の横で右クリックし、「プロパティ」を選択する。
 - (iii) 「全般」タブで「詳細」ボタンをクリックし、「属性の詳細ダイアログボックスが表示される。
- (図 4)
- (iv) 「内容を暗号化してデータをセキュリティで保護する」にチェックを入れ「OK」をクリックする。
 - (v) フォルダを暗号化するように設定した場合は、そのフォルダだけを暗号化するかフォルダに含まれるすべてを暗号化するかのどちらかにチェックを入れ、「OK」をクリックする。(図 5)

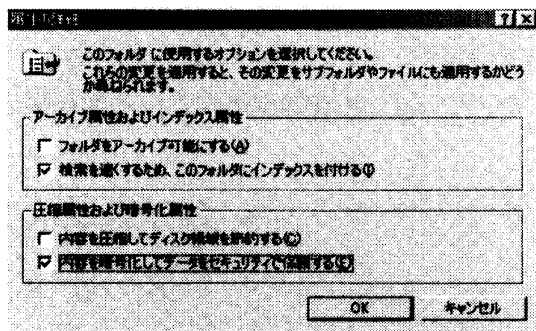


図4. 「属性の詳細」ダイアログボックス

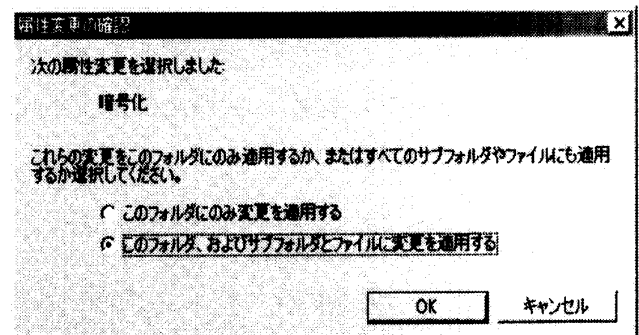


図5. 「属性変更の確認」ダイアログボックス

8. Misty を使った暗号ソフトのインターフェース画面

暗号アルゴリズム Misty を使った暗号ソフトのインターフェース画面は図6のようになる。これは VC++ で開発されておりメール送信、暗号化、鍵管理が主な機能となる。ウインドウ中の右のウインドウで、文章を送信し、左のウインドウで鍵を選択し、暗号化する。今後はデジタルコンテンツ配布、デジタル認証書発行と管理、ファイル暗号化などの機能も付けて実験を行う。その際開発において使用する関数は以下の表の通りである。

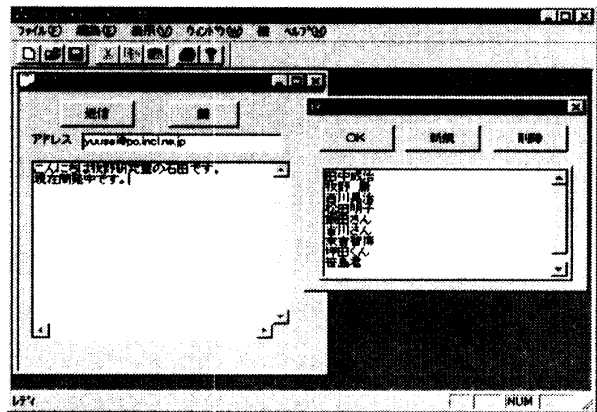


図 6 インターフェース画面

処 理	関 数 名	機 能
アルゴリズム	M_CreateAlg	アルゴリズム情報の設定
	M_CopyCryptoInfo	アルゴリズム情報の複写
	M_DestroyAlg	アルゴリズム情報の破棄
鍵の操作	M_SetSysInfoBin	鍵生成の条件とするシステム情報の設定(バイナリ値)
	M_SetSysInfoInt	鍵生成の条件とするシステム情報の設定(整数値)
	M_SnoopSysInfoBin	鍵生成の条件とするシステム情報の参照(バイナリ値)
	M_SnoopSysInfoInt	鍵生成の条件とするシステム情報の参照(整数値)
	M_GenerateKey	鍵の生成
	M_SetKey	鍵の設定
	M_ObtainKey	鍵の取得
	M_AgreeKey	鍵の交換
	M_GetKeyInfo	鍵情報の取得
	M_PutKeyInfo	鍵情報の設定
	M_GetKeyElemBin	鍵データからの要素データの取得(バイナリ値)
	M_PutKeyElemBin	鍵データへの要素データの設定(バイナリ値)
	M_GetKeyElemInt	鍵データからの要素データの取得(整数値)
	M_PutKeyElemInt	鍵データへの要素データの設定(整数値)
	M_InitKeyInfo	鍵データフォーマットの初期化
	M_KeyInfoLen	鍵データの長さ取得
	M_SnoopKeyInfoProperty	鍵データフォーマット情報の取得
メッセージ 処 理	M_OpenContext	メッセージ処理開始の宣言
	M_ProcessMessage	メッセージの処理
	M_GetResult	メッセージ処理結果の取得
	M_SetVerifyingValue	検証用データの設定
	M_VerifyResult	検証用結果の取得
	M_CloseContext	メッセージ処理終了の宣言
そ の 他 の 処 理	M_Srand	乱数の種の設定
	M_Rand	乱数の取得
	M_GetErrorNum	詳細エラー番号の取得

表1.Misty の暗号ライブラリが提供する関数

9. セキュリティシステムを使った応用例

セキュリティシステムを使った応用例として決済があげられる。電子商取引で重要となってくる決済だが、手軽に扱えるという点から事前の手続きや、専用ソフトのインストール不要なシステムを考える場合、どうしてもセキュリティ対策が甘くなりがちになる。そこで決済エージェントでは

- (a) データ暗号化通信には MISTY を採用
- (b) 決済方法はクレジットカード番号の事前登録をする。
- (c) 本人認証には、本人で決めた項目を設ける

という 3 つの点で、専用ソフトインストール不要のシステムを考えた。本人認証に、本人しか知らない項目を設けるという方法は、アメリカなどで本人認証に多く採用されている方式である。また、情報として登録するのは、郵便番号、住所、氏名、電話番号、生年月日、メールアドレス、ID、パスワード、そして本人認証である。住所、クレジットカードの追加登録などができるが、その際に、あらかじめ自分できめた ID、パスワード以外に本人認証例として(まきの研究室)の回答を入力することにより、はじめて自分の情報にアクセスできるというものである。また、これは利用者からの観点からしか見ておらず、店舗側から見た観点も考慮して改良していく。

10. 結 論

本論文ではサイバー情報セキュリティの暗号技術・認識技術を考察し、続いて実験(I)認証方法比較分析、実験(II)ファイル暗号化分析を行った。最近の高度情報化社会では“セキュリティ技術を破る技術”も日々進化しており、完全なセキュリティシステムの構築は難しい。だがそれに伴い新しいセキュリティシステムの設計開発技術も日々進化している。そういった技術を研究し、より使いやすく、強度の高いセキュリティシステムを今後も構築していきたい。なお、サイバー情報セキュリティには“経済性”が重要な要素となるが本研究では、今後の課題として経済効果の上がるセキュリティについて研究を進めたい。

参考文献

- 1) 山口 英・鈴木裕信：「情報セキュリティ」、共立出版
- 2) 田晃一・峰岸和弘・船木春仁：「eセキュリティ」、ダイヤモンド社
- 3) Mitsubishi Electric Corporation：「Misty Guard<TRUSTWEB>マニュアルセット」
- 4) 武田圭史・磯崎 宏：「ネットワーク侵入探知」、Soft Bank パブリッシング株式会社
- 5) 和田 秀男：「コンピュータと素因数分解」、遊星社
- 6) 電気関係学会北陸支部：「平成13年度 電気関係学会北陸支部連合大会 講演論文集」

(平成13年12月6日受理)