



株式会社ピー・ユー・ジー
RSAプロジェクト代表
浅田 一憲

インターネットや将来の情報スーパーハイウェイに欠かせない技術の1つに情報セキュリティがある。情報セキュリティ技術は、悪意のある人がいる環境にあっても、安心してネットワーク上で重要な情報のやり取りを可能にする基本的な技術である。ネットワーク上では、「盗み見」、「なりすまし」、「しらばくれ」、「改ざん」などが行われやすいが、情報セキュリティ技術を駆使すれば、そうした悪事も防ぐことができる。誰もが安心して積極的に自分の情報を発信でき、また信頼して相手の情報を受け取ることができる。今回は情報セキュリティ技術の最新動向について解説してみたい。

情報セキュリティ技術の要 RSA

【第3回】セキュリティ技術の最新動向

開かれたネットワークを
つくるための技術

情報セキュリティ技術の基本は暗号技術である。皆さんは「暗号」と聞くとどんなことを思い浮かべるだろうか？ 軍事目的や警察無線などで暗号が使用され、秘密の重要情報をなるべく敵や一般市民から隠そうとする「暗い技術」というイメージを持っていないだろうか？ そもそも暗号という単語自体に「暗い」という文字が入っている。暗号の研究者なんてスパイか何かと組んでいかかわしいことをやっているように思える

だろう。何を隠そう、筆者自身もついこの間までそう思っていた。

しかし、ネットワーク社会で使用される情報セキュリティ技術は、このような消極目的で使用されるだけではない。それどころか、最近はむしろ自分の情報を積極的に発信すると同時に、相手の情報も積極的に活用するために使用される。暗号技術は、ネットワーク上の多くの人々との信頼関係を築き上げるための基本となる技術であると考えてほしい。ネットワークや電子媒体を活用し、情報を受発信したり、創作活動を行ったりすることを通じて自らこの大

きな社会で活躍するときに使用する非常に積極的に明るい技術が、これからの暗号技術、情報セキュリティ技術である。

セキュリティ技術は
コストを下げる

ネットワーク上での情報やサービスのやり取りを考えたときに、多くの場面で情報セキュリティの技術が利用されるようになると思われるが、どうしてこのような技術が必要なのだろうか。ここで基本を振り返ってみよう。セキュリティなんてなくても実際は大した問題にはならないからあまり重



要ではないと考えている人も中にはいるようだ。たしかにセキュリティがなければいかにどうにかなる場合が多い。しかし、たいいていの場合、情報セキュリティ技術を使用するいちばん大きな理由は、それが絶対に必要だからではなく、コストが下がるからなのである。情報セキュリティ技術を使用すると減らすことのできるリスクが多く存在し、それらのリスクは金銭に換算することができる。ネットワークで商売を行う人は、リスクを保険会社に買ってもらったり、自分で負担して、その分を商品の単価に上乗せして消費者に転嫁したり、自分の利益を減らしたりしている。情報セキュリティ技術を使用すると、リスクすなわちコストを減らしたり場合によってはゼロにしたりすることができるのだ。情報セキュリティ技術は、ネットワーク社会やデジタル社会でのコストダウンのための技術である、と考えてもよいだろう。

重要性を増す「電子印鑑」

さて、情報セキュリティ技術が「盗み見」、「なりすまし」、「しらばくれ」、「改ざん」の問題を解決でき、さらに将来に向けて、電子決済、電子出版、遠隔治療、教育、デジタルデータの著作権の管理や電子

現金、その他さまざまな分野で使われていくとすると、いちばん多く使用される技術は「電子印鑑」の技術であろう。電子印鑑は、自分の発信した情報について、「確かにその内容を自らの意志で発信した」ということを証明する技術である。逆に言えば「なりすまし」、「しらばくれ」を防止し、「改ざん」を検出できるということになる。電子印鑑の技術は、アメリカのRSA Data Security, Inc. (RSADSI) とVeriSign, Inc. (VeriSign) のものが最も進んでおり、世界のデファクトスタンダードとなっている。以前に本誌(1995年9月号・11月号)でも、RSADSIとVeriSignの技術について解説した(図1)。情報スーパーハイウェイを走る車の運転免許証にあたるのが電子印鑑証明書(Digital ID)である。VeriSignの電子印鑑証明書の仕組みが、本年の3月頃に改良され、より使いやすく便利になる予定だ。そこで、次にそれについての解説をするとともに、情報セキュリティの文字どおり鍵を握る会社の日本での活動についてもレポートしよう。

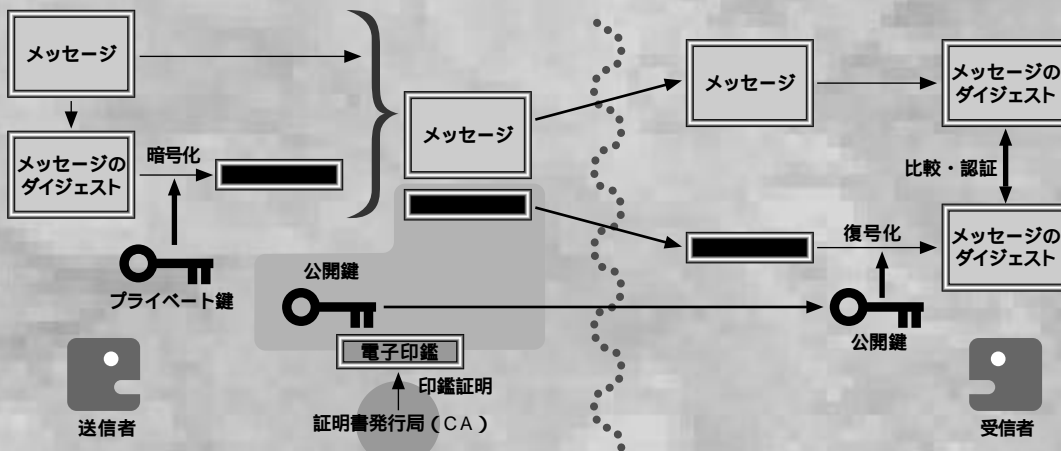
新しい電子印鑑証明書の仕組み

一般の個人や企業に電子印鑑証明書を発行する公共サービスには、「クライアント

用電子印鑑証明書発行サービス」と「サーバー用電子印鑑証明書発行サービス」がある。また、特定の企業やグループ内でのみ有効な電子印鑑証明書を発行したり、発行システムを販売するプライベートサービスもある。公共サービスで発行された証明書は、いろいろな人が多くの目的で使用する可能性がある。そこで、VeriSignの電子印鑑証明書も、基本的には日本の役所が発行するのと同じように、個人や団体がどこに何という名前が存在しているということだけを証明するようになっている。その人がまっとうな職についているかとか、前科はないかとか、経済状態はどうかなどといったことは、いっさい証明しない。それらのことは、電子印鑑証明書を使用する人や会社が、別に調査すべき事柄と考えられている。もちろん、それらのことについて証明する証明書を発行したい場合は、プライベートサービスを利用すればよい。

なお、以前は、Digital IDのことを「Digital Certificate」、クライアント用電子印鑑証明書のことを「個人向け電子印鑑証明書」、サーバー用電子印鑑証明書のことを「会社向け電子印鑑証明書」と呼んでおり、本誌でもそれらの用語を使用していたが、概念が統一されて呼び名が変わったので、ここでもそれに準じて話を進めたい。

図1：情報セキュリティ技術のしくみ



- ① 送信者はプライベート鍵と公開鍵を1組持っている。
- ② 送信者はプライベート鍵でメッセージのダイジェスト(特徴的なデータ)を暗号化し、メッセージと公開鍵と合わせて送る。
- ③ 受信者は受け取った公開鍵でダイジェストを復号化する。
- ④ 受信者はメッセージから独自にダイジェストを作成する。
- ⑤ 受信者は2つのダイジェストを比較し、同じものであればメッセージは送信者が作成したものと分かる。

① クライアント用印鑑証明書発行サービス

電子印鑑証明書（Digital ID）がクラス分けされた。今まで1種類しかなかった電子印鑑証明書であるが、新しい仕組みでは電子印鑑証明書の保証のレベルによって4つのクラスに分かれる（図2）。保証レベルというのは、個人と発行する電子印鑑証明書との関連性をどこまで保証するかということである。言い換えれば、証明書発行局（Certifying Authority：CA）が、「その人が本当にそういう名前でその住所に存在しており、印鑑証明書を請求している人と同一人物かどうか」ということをどれだけ詳しく確認を行うかという証明書の確かさにレベルができたということである。

（クラス1）

電子印鑑証明書は、名前または電子メールアドレスの唯一性を保証する。クラス1の電子印鑑証明書は、簡易なWWWブラウザや電子メールで使用され、インターネットを通じてリクエスト発行してもらうことができる。電子メールによるやり取りを通じて、そのメールアドレスの人が世の中にただ1人実在することを確認し、証明書の発行を行う。PGP*のようなPDSメールソフトで事足りている人は、このク

ラスの証明書を利用するのがよいだろう。

（クラス2）

クラス2の電子印鑑証明書を発行する際、CAは申し込み時に登録した名前や住所、その他の個人情報が正しいかどうかを第三者機関を通して調査する。アメリカでは個人情報にアクセスできるデータベースなどが比較的安い値段で入手できる。クラス2の発行時には、そのような民間のデータベースを複数使用し、その人の名前や住所などの個人情報を確認するものと思われる。クラス1の証明書は、特定のメールアドレスなどを持っている人が実存することだけが保証されたが、クラス2では、個人情報の正当性を保証できる。会社間の電子メールやエレクトリックモールでの買い物などに使用することができるだろう。

（クラス3）

申し込み者が本当に存在することと個人情報の正当性を、クラス2より高いレベルで保証する。商取引などで必要な高いレベルの個人特定保証を行う。発行には、公証人のサインや住民票、銀行口座番号などの公的書類やそれに準ずるレベルの書類が複数求められる。会社間の電子メールや電子バンキング、電子モールで高額な買い

物を行う場合や会員制の情報サービスを利用する場合などに使用する。

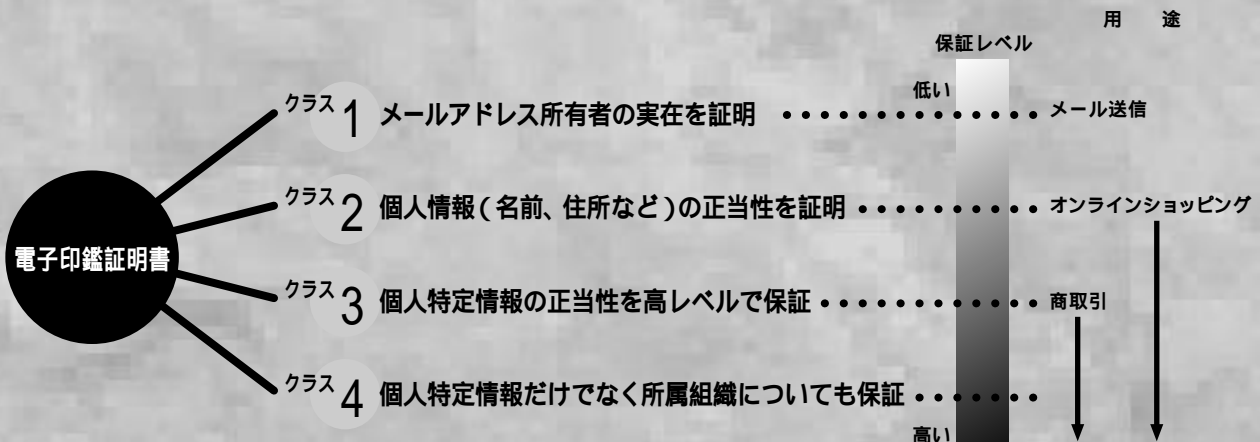
（クラス4）

本人の実在に加えて、個人情報や勤めている会社などの所属組織などについても独自調査を行って保証する。

本来、CAが必ず正しい電子印鑑証明書を発行するのであればこのようなクラス分けなどは必要ないのだが、証明書の絶対的な正当性を保証しようとする発行までに多額のコストや時間がかかる。クレジットカードには信用の度合いに応じて学生カードや一般カード、ゴールドカードなどの種類がある。今回、電子印鑑証明書でも簡単に安く発行してもらえて本人の確認が簡易なものから、時間と高額な発行料がかかるが高レベルな正当性の保証があるものまで用意されたことで、使用する人の目的に応じてレベルの選択ができるようになった。CAに唯一絶対の正確さを求めるより、選択の幅が与えられたほうが、利用者にとっては便利なのが多いと思う。今回のVeriSignの仕組みの変更は、ネットワーク社会のニーズに素早く対応した措置であり歓迎したい。

Netscape Navigatorは、間もなくクライアント用の電子印鑑証明書をサポートする。

図2：電子印鑑証明書の4つのクラス





ユーザーはオンラインでVeriSignから電子印鑑証明書をリクエストし、オンラインで受け取ることもできるようになる。これにより、Netscapeは、電子モールでの買い物や、Secure MIMEフォーマットのセキュリティ電子メールの送受信などができるようになる。

日本では、少し前まで、著者の属する株式会社ビー・ユー・ジーの子会社の株式会社フィクスがRSADSIのライセンスを受け、電子印鑑証明書発行公共サービスを行ってきたが、1995年10月より同じく株式会社ビー・ユー・ジーの子会社の株式会社バイスがCA業務を引き継いだ。株式会社バイスは、今度はVeriSignのライセンスを得て証明書を発行している。今までの電子印鑑証明書は、新しい仕組みに当てはめるとクラス3に相当する。株式会社バイスでは引き続きクラス3の電子印鑑証明書を一般の人々に発行していく。

② サーバー用電子印鑑証明書発行サービス

クライアント用電子印鑑証明書発行サービスは、WWWブラウザや電子メールを使用する個人向けに電子印鑑と電子印鑑証明書を発行するサービスであるが、VeriSignでは、人ではなく物に対しても電子印鑑証明書を発行している。特に

Secure Socket Layer (SSL) や Secure HTTP (S-HTTP) を使用しているWWWサーバー上で、クライアントとクレジットカード番号などの重要な情報をやり取りするために使用されている。具体的には、Netscape Commerce Server やStarNineのWebSTAR、IBM Internet Connection Server、CompuServeのWebServerのほか、WebSite、Open Market、Internet Factoryなどの多くのWWWサーバーでサポートされている。VeriSignは、現在サーバー用印鑑証明書はクラス3を発行している。アメリカでは、サーバーを立ち上げている会社の州が発行するビジネスライセンス番号や社長がサインしたレターなどが必要であるが、日本では会社の登記簿謄本や印鑑証明書などの書類が必要になる。Netscape Commerce Serverを始めとするサーバー用印鑑証明書は、世界中でVeriSignだけが発行している。日本では、株式会社バイスが1995年3月より発行受付業務を行っている。このように、CAであるVeriSignとユーザーの間に立って書類や印鑑証明書の受け付けや引き渡しなどを行う機関のことをLocal Registration Authority (LRA) といい、株式会社バイスは海外CAの第1号に引き続き、LRAの第1号となった。

③ 電子印鑑証明書発行システムの変更

今まで、電子印鑑証明書はCIS (Certificate Issuing System) というシステムを使用して発行されていた。CISは、鍵をストアするための攻撃対抗容器 (Tamper Resistance Module) であるCSU (Certificate Signing Unit) とMacintoshまたはWindowsNT、Oracleのデータベースで構成されている。1996年春より、CISはもっとも高機能で柔軟性のあるCMS (Certificate Management System) に代わる。CMSは、メインコンピュータにSUNなどのUNIXマシンを使用し、ネットワークで接続され、インターネットを通じた電子印鑑証明書の請求受け付けや発行ができるようになった。また、有効期限内であっても何らかの理由で無効になった電子印鑑証明書の一覧表である「電子印鑑証明書廃止リスト (Certificate Revocation List、CRL)」のネットワークによる問い合わせに応じることができる。CRLは、引っ越しや結婚などで住所や名前が変わって新たな証明書を発行した場合など、証明書の有効性を確認するのに役立つ。高額な商品の購入時などにアクセスされることになるだろう。

*PGP (Pretty Good Privacy) : インターネット上の電子メール用の暗号化システム。
RSAの技術に基づく公開鍵方式が使われている。



日本ベリサイン株式会社の設立

日本のエレクトリックコマース技術は、世界でダントツに進んでいるアメリカに続いて世界で第2位の位置をなんとかキープできている状態である。特に情報セキュリティ技術に関しては、ヨーロッパより進んでいる。特にこの1年は、通産省や郵政省の予算に関連してエレクトリックコマースブームと呼ぶべき現象が起こっており、ヨーロッパよりかなり進んでいる。ネットワーク社会に国境はない。ネットワーク社会は距離と時間の差がなくなる社会であり、ある時点で世界のどこかで起こっていることは、すなわち今ここで起こっていることと考えることができる。技術的な面でも文化的な面でも世界がある意味で画一化され、ショッピングでも銀行でも何でも最も便利で条件のよいところが多く使用されるようになる。日本の店から日本の消費者が物を購入するときでも、アメリカやシンガポールの銀行を使用して決済するなどということは、日常的に行われるようになるだろう。

このような背景を踏まえて、日本でも世界的に競争力のある電子印鑑技術を利用できるようにするために、米国VeriSignは、NTTグループと共同で1996年2月22日、日本ベリサイン株式会社を日本国内に設立した。VeriSignの子会社が設立されるのは世界でも初めてのことであり、ベリサイン株式会社は、電子印鑑証明書の発行サービスや、プライベートなCAの構築のためのシステム販売などを行い、電子印鑑証明書の技術の普及に尽力することになるだろう。将来的には、広い分野の日本企業から出資者を多く募り、中立な立場の信頼のある会社になることを期待している。

RSADSIのロゴ戦略

RSADSIは、自社のライセンスを受けているソフトウェアが、RSA純正の優れた暗号モジュールを使用していることをアピールできるようにするため、製品に「Genuine

RSA」というロゴを付けて販売することを推奨することにした(図3)。ちょうど、Intelが「Intel Inside」というロゴを製品に付けることを推奨し、縁の下の力持ち的な存在であるCPUメーカーの名を一躍有名にしたのと同じように、一般ユーザーにRSAの名前をもっと知ってもらい、ある種のブランドイメージを植え付ける効果を狙っている。

また、MicrosoftやLotusなどととも普及を促進しているセキュリティ対応の電子メールの規格である「S/MIME」や、1995年12月にできたばかりのセキュリティ対応WAN(Wide Area Network)の規格である「S/WAN」についても、それぞれロゴを用意してイメージ戦略を行っている(図4)。今後、Netscape NavigatorやLotus Notes、CC:Mail、Microsoft Mailなどの主要な電子メールソフトウェアは、次々にS/MIMEに対応し、ダイヤルアップルーターやリモートアクセスサーバーなどのネットワーク機器も、次々S/WANに対応していくと思われる。これからはセキュリティ機能は必要不可欠であるので、これらのロゴをあちらこちらで目にする日も近いだろう。

アメリカの暗号技術の 日本への輸入について

ピー・ユー・ジーは、1995年9月末に、今までアメリカ国外に輸出が認められていなかったRSADSIの暗号ソフトウェア開発ツールキットのBSAFEとTIPEMの輸入に世界で初めて成功した。BSAFEは、RSA、Diffie-Hellman、Bloom-Shamir、DES、DESX、RC2、RC4、MD、MD2、MD5などの暗号アルゴリズムのライブラリーであり、主要なアルゴリズムのほとんどをカバーしている。残念ながら我々が輸入できなかったBSAFEには、Triple-DESだけは含まれておらず、その部分だけアメリカでライセンスされているものとは違っている。MicrosoftのWindows95やNT、Lotus Notes、Novell NetWare、Oracle SQL*Net、WordPerfect InForms、General Magic Telescriptなどの主要ソフトウェアはすべてBSAFEを使用して開発されており、ライセ

ンスを受けている。また、TIPEMは、セキュリティ通信とエレクトロニックコマース用ソフトの開発ツールキットで、暗号技術の応用ライブラリーが多く含まれている。PKCS/PEM/X.509などのスタンダード規格で定められている電子印鑑証明書やX.400 '88のセキュリティ規格であるRFC1421-1424のInternet Privacy-Enhanced Mail(PEM)をサポートできるモジュールなどがある。NTTエレクトロニクス株式会社(NEL)も、ピー・ユー・ジーに続いてTIPEMの輸入に成功し、日本でも本格的にセキュリティ技術入りソフトウェアを開発できるようになった。

残念ながら、BSAFEもTIPEMも、ツールキット自体の転売は認められていないので、日本企業が自由にセキュリティソフトを開発できるようにはなっていないが、ピー・ユー・ジーに開発を委託することによって間接的に開発を行うことができる。しかし、開発したソフトウェアを販売するときは、さらに2つの許可を得る必要がある。

1つは、商品化することに対するアメリカ政府からの輸出許可の取得である。この許可は正確にはRSADSIがアメリカ政府から取得する。取得には、輸出先、ソフトウェアの目的や販売数、使用している暗号の種類や強さの情報を添えて申請しなければならない。アメリカ政府は1995年の8月以降、一部に対しては暗号技術の輸出許可条件を緩和しており、56bitのDESに関しては16bitだけを、64bitのRC4の場合は24bitだけを鍵供託(Key Escrow)することにより、40bit超の鍵サイズの暗号入りソフトウェアも輸出を認めるケースも出てきている。RSADSIは、アメリカ政府からピー・ユー・ジー向けにManufacture Licence Agreement(MRA)を取得しており、ピー・ユー・ジーが相手のRSADSIのセキュリティ技術の輸出販売許可は一定の条件下でたいていの場合認められる。アルゴリズムもDESやRC4に限らずほとんどのものを輸入して商品に含めることが可能である。

もう1つの許可は、RSADSIからのライセンス取得である。ピー・ユー・ジーは



RSADSI から包括的なセキュリティ技術のライセンスを取得しており、RSA がアメリカ企業にライセンスを行っている技術に関しては、すべてライセンスを受けることができる。また、OEM ライセンスも取得済みで、第三者のセキュリティ入り製品の一部をビー・ユー・ジーが開発して提供し、第三者ブランドで商品化することも問題なく行える。特に、BSAFE と TIPEM に関してはオブジェクトコードに続いてソースコードライセンスも取得しており、特殊なプラットフォームでのセキュリティソフトウェアの開発なども行うことができる。BSAFE と TIPEM は、クライアント用とサーバー用にライセンスが分かれており、クライアント用はサーバー用よりかなりライセンス料が安い。

このように、努力の甲斐があって、日本でも徐々にアメリカと同等なレベルのセキュリティ技術が使用できるようになってきた。1995 年は、日本のエレクトロニックコマースにとって大きな意味を持つ1年であったと言える。

RSA 暗号方式に対する新攻撃法

1995 年 12 月 7 日、暗号コンサルタントの Paul C. Kocher は、RSA 暗号方式などに対する新方式の攻撃方法 (Timing Attack) を発表した。Kocher は、RSA の計算、 c^d

$\text{mod } n$ の c^d 部分のインプリメンテーションに注目し、 d (すなわち暗号鍵の一部) を 2 進数で表したときに値が 1 になるビットの数と、 c^d を計算するのに要する時間が比例するというを発見した。RSA 暗号方式を計算するルーティンが特定できれば、そのルーティンに飛び込んでから抜け出すまでの時間を一定期間以上計測することによって、統計的に鍵の一部がある程度予測できる (何ビットが 1 で何ビットが 0 か)。また、この方法は RSA 以外の多くの暗号方式にも使用できる。Kocher の方法は、これまでの RSA 暗号方式に対する攻撃法とは違ってインプリメンテーションに対する初の理論的攻撃法であり、軽視することはできない。対抗方法は、① c^d の計算ルーティンに何ミリ秒かの無駄なループを入れて計算時間を一定にする、② ブラインドシングネチャー ($r^{-1}(cr^e) \text{ mod } n$) を使用して元の平文自体を変えてしまい統計的手法を使用できないようにする、③ 値が 1 になるビットの数によって計算時間が変わらない c^d の計算インプリメンテーションを行う、などが考えられる。この攻撃法の発見が RSA 暗号方式にとってどの程度脅威であるかまだ結論は出せないが、著者自身の見解としては、さほど脅威ではないと考えている。Kocher の方法はソフトウェア中の c^d の計算部分を正確に特定し、さらに実際に暗号演算が行わ

れる瞬間を捕らえ、高い精度で実行時間を計測するといったことを長い間続けなければならない。理論的には攻撃できて、実際にコンピュータの中で恒常的に動作し、秘密裏に暗号ルーティンを監視するウィルスのようなソフトウェアとしてインプリメントするのは難しい。また、上記の 3 つの解決方法の中で①と②は簡単に実現できる。③についても中国人剰余定理を使用すれば処理時間は今よりはビット依存しなくなる。よって今回のことで RSA 暗号方式は大事には至らないと確信する。しかし、今までまったく考えてもいなかった攻撃法もあるのだということを再認識させられ、セキュリティシステムに油断は禁物であるということを変更して勉強させられた。

日本 RSA 株式会社の設立

ベリサイン株式会社同様、本家の RSADSI も 2 月 8 日に日本法人を設立した。詳しい活動はまだ未定であるが、セキュリティ技術のライセンス、セキュリティ入り製品の OEM ソリューションの提供、アメリカの RSA Laboratory のような研究活動が予定されており、セキュリティ技術はいっそう利用しやすくなるだろう。

(本稿に関するお問い合わせは、rsaproj@bug.co.jp までお願いします)

図 3 : 「Genuine RSA」のロゴ



図 4 : 「S/MIME」と「S/WAN」のロゴ





[インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

株式会社インプレスR&D

All-in-One INTERNET magazine 編集部

im-info@impress.co.jp