# 総論—社会を変革する暗号技術

岡本　栄司

## 1. はじめに

インターネットを核とするITの進展により，電子社会の到来が身近に感じられるようになってきている．銀行の決済や買い物がインターネットで可能になっており，役所では電子申請やICカードによる住民情報登録が広まりつつある．また，医療機関においてはICカードによる電子カルテなども一部始まっている．さらには音楽や画像などのディジタルコンテンツもインターネットを通じて入手できるようになっている．

ナップスターの音楽配信システムに対しては，アメリカ連邦地裁が営業差し止めの仮処分を下したため(その後，高等裁ではその執行を延期する処分を下した)，その勢いが多少鈍ったが，趨勢に変化はないであろう．

最近の通産省の調査によると，わが国におけるディジタルコンテンツ配信による市場規模は1999年で85億円だそうで，5年後には5,280億円規模になるそうである．

このように，インターネットの広がりは社会を変えつつある．その本質は，今までのMass Communicationによる一方向性通信かつマスメディア対大衆に対して，Personal Communicationによる双方向性かつ個人対個人にある．個人情報の伝わる範囲が格段に広がり，しかも瞬時に伝わるのが特徴となっている．情報収集でも広範囲から短時間に情報が集められる．

こうなると，個人のプライバシーを侵害することも容易となってくる．このため，情報セキュリティの重要性が一般にも認識されるようになってきた．

一方で，ネットワークに対するアタックも多くなっている．今年に入ってからもWeb Pageの書き換えや，I Love Youウィルスなどがあった．被害からすると，今までは，ハッカーの個人的な興味による侵入が多いが，今後はテログループや国家によるアタックも予想され，強力な武器になりつつあると見られる．

このため，これらからのアタックを防ぐためのセキュリティ技術の重要性が叫ばれている．特に，その中でも核となる暗号技術の必要性が高まっている．現在，暗号は急速な普及期を迎えようとしており，政府の取り組みにも一段と力が入ってきた．

そこで，ここではまずセキュリティ対策の考え方について述べ，次に暗号技術を簡単に紹介する．そして，その暗号が実際どのように使われているのかを例をあげて解説する．

## 2. 電子社会への進展と安全性に対する脅威

コンピュータが便利になって，家庭にもかなり普及してきている．遠くの人と電子メールで連絡しあったり，いろいろなホームページを見て買い物をしたり，音楽を楽しんだり，あるいは求職・求人活動もネットワークを通じて行われている．こうなると，もうコンピュータなしでは生きていけなくなる．

しかし，一方では，官公庁のホームページが盛んにアタックされて，いとも簡単にホームページが書き換えられてしまったり，コンピュータウィルスという伝染性のあるプログラムが，勝手に他人のコンピュータに入り込んできて中身を変えてしまっている．

こうなると，コンピュータも便利だけど怖いものでもあると言わざるを得なくなる．このままではネットワークでオンラインショッピングをしようとしても安心してできない．実際にこのような人騒がせなことをするのはごく限られた人であるが，わずかな人数でも全世界に影響を及ぼすことができるのがコンピュータネットワークのいいところでもあり悪いところでもある．

現在のアタックは次のような構図になっているようである．まず，コンピュータに詳しい技術者がアタックツールを作成してはそれを公開して，誰でもただで

おかもと　えいじ　東邦大学　理学部
〒274-8510 千葉県船橋市三山2-2-1


© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

使えるようにする．これ自体は違法とはいえないところが問題であり，特に，海外だと道義的にどうのこうのといってもはじまらないところがある．次に，それらを使って実際にアタックする人たちがいる．通常は作成者ほどコンピュータに詳しくないが，アタックツールを扱う程度には詳しい人たちである．単なる興味や何らかの不満をもって他のコンピュータに侵入するが，嵩じると作るほうに回ることもある．

いくつかのアタック例を示そう．

最近のホームページ書き換えアタックはオーバーフロー法といわれるものである．一度に大量のデータをいろいろなところから送り込んで，ホームページのコンピュータがその処理に追われている間に，別の命令を送り込んでそれを実行させてしまう．本来は権限あるユーザからの命令しか実行しないが，混乱に紛れてその権限チェックが終わる前に実行させてしまうものである．

他のアタックとしては，ダイレクトメールを他の差出人の名前で大量に出すスパムメールというのもある．宣伝メールなどを他のコンピュータを通して沢山の人に出すものである．中継となったコンピュータはその膨大な発送処理をさせられるのでたまらない．また苦情も舞い込むことになる．

コンピュータウィルスについては，われわれユーザ自身が気をつけなければならない．メールの添付ファイルなどに添付されて送られて来るからである．メールを処理するコンピュータ（メールサーバ）はメールの中身まで開封してコンピュータウィルスがついているかどうかをチェックするわけにはいかないのである．

スキミングというクレジットカードを対象にしたアタックも増えている．これは，販売店のある人が客のカード番号をレジでさっと読み取り，その情報を更に別な人が集め，新しいカードに記入して売りに出そうというものである．この被害は結構増えつつある．

## 3. 情報セキュリティ対策の考え方

対策には事前対策と事後対策の二通りがある．また事前対策には未知アタック防禦対策と既知アタック防禦対策がある．未知アタック防禦対策はネットワークソフトウェアのセキュリティホールを見つけてそれを潰していく方法である．既知アタック防禦対策は，どこかあるところでコンピュータがアタックされた場合に，それに対する対策を考案し，考案された対策を他のところのコンピュータに導入してそのアタックを予防するものである．コンピュータウィルスに対するワクチンはその代表例であろう．

事後対策はシステム監査（ログ）や保険などである．アタックを記録されていることがわかるとアタックにブレーキがかかるので，かなり効果がある．緊急対応センターによる援助も事後対策と考えられる．情報セキュリティ対策は，他の技術と異なってシステム破りとそれからの防禦の繰り返しになるので，どうしても破られたときの対策を考慮しておくことが不可欠となる．この意味でも，事後対策は重要である．

アタックはこれからも増えることがあっても減ることはない．例えるならば，風邪と同じようなもので，絶滅させるのは無理である．いかに効率的かつコストパフォーマンスのいい薬を作れるかがカギである．万能薬はありえず，具体的なアタックごとに薬を調合することになる．

実際にこれらの対策に使われる技術には，

・事前対策—暗号/認証，電子透かし，耐タンパー

・事後対策—セキュリティポリシー，システム監査

などがある．これらが，実りある対策となるためには，さらに

・非技術的対策—倫理・教育・啓蒙，情報保険，法制度

が必要となる．また，セキュリティ対策の普及には

・安心感—一般ユーザの不安感を払拭する仕組み

も必要となる．すなわち，大切な情報が本当に見られていないのか，消えてしまわないのか，という不安感を払拭して安心して使えることを実感できる仕組みである．

これら全体を含めた概念がInformation Managementといい，技術でカバーできない運用管理などの部分まで含めて問題解決を図ろうとするものである．

## 4. セキュリティ対策のための基本技術

セキュリティは複合的なシステム技術である．そこに使われる基本技術をごく簡単に紹介する．

### ◉暗号/認証

暗号や認証は情報セキュリティの核となる技術であり，著作権保護などいろいろな場面での基礎技術になっている．メッセージの秘匿性，正当性および完全性の確保に利用される．現在よく用いられるのは公開鍵暗号系である．RSA暗号/署名が代表例であるが，DSS署名，ElGamal暗号/署名，ESIGNなども用いられている．暗号/認証については次節で改めて述べ


© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

る．

●電子透かし

コンテンツの著作権保護方式として，多くの電子透かしが提案されている[2, 7]．電子透かしとは，コンテンツに人間が感知できない形で透かし情報と呼ばれる別な情報を埋め込むことである．透かし情報に著作権情報などを入れれば著作権保護になる．

電子透かしとなるための条件として，透かし情報を入れてもコンテンツの品質が劣化しないこと，透かし情報の除去が困難なこと（無理して除去するとコンテンツの品質が著しく劣化する），編集・加工操作によっても透かし情報が残ることがあげられる．

電子透かしにはいくつかの方式が提案されている．分類の観点としては

・読み出し時にオリジナルが必要か否か

・鍵情報を必要とするか否か

などがあり，当然のことながら，オリジナルも鍵も不要なものが使い勝手はいい．しかし，通常セキュリティ強度が下がるので，トレードオフとなっている．その他に，

・時間空間に埋め込むか周波数空間に埋め込むか

・埋め込み情報量の多さ

によっても分類される．周波数空間ではDCT，FFT，Wavelet変換などが利用される．

電子透かしの商用ソフトも出ており，わが国ではIBMやコーワなどが販売している．

著作権保護方式として電子透かしを使うとすると，どうしても著作権使用などによる課金処理過程が含まれるようになる．そこで，次の超流通と結びつき易くなり，現にアメリカのInterTrust社が超流通を組み込んだDigital Rights Management Platformを出している．

●超流通

森亮一により提案された著作権保護方式である[3]．ソフトウェアのコピーはいくらでも許すが，ソフトウェアを実行するときに課金するという方式である．ソフトウェアの著作権保護方式として提案されたが，原理的にはどんなコンテンツにも適用できるものである．

ソフトウェアには課金に関する情報が含まれ，実行時に課金処理を行うシステムが必要となる．Pay per View方式の有料TVに似た概念であり，同様に利用者でもごまかせないような高セキュリティ機能が要求される．すなわち，課金処理部分を変えられないような耐タンパー性が求められる．

●耐タンパー

著作権保護方式に限らず，情報セキュリティを守るシステムは，ハードウェアであれソフトウェアであれ，改竄や変造に耐え得るように作られていなければならない．例えば，超流通の課金処理部分が変造されて課金料が減らされると事業が成り立たなくなる．また，DVDをパソコンでもコピーさせずに見られるようにするために，CSS（Content Scramble System）と呼ばれる暗号方式が耐タンパーなソフトウェアとして実現されている．

ハードウェアで耐タンパー性を保つのはそう困難ではないが，ソフトウェアで耐タンパー性を保持するのは容易ではない．例えば，前述したDVDの不正コピー対策用システムのCSS方式は耐タンパー性ソフトウェアにもかかわらず，ハッカーグループはCSSを解析し，Linux用にDeCSSというソフトウェアを作成してコピーも可能にしてしまった．実際にはCSSは暗号化されているが，その鍵の管理が一部でずさんだったために鍵がばれたのがきっかけとなって，解析されてしまったのである．なお，DeCSSの使用は禁じられ，またハッカーたちは家宅捜索を受けたようである．

●リニューアルシステム

著作権保護方式に限らず，情報セキュリティ技術では，アタックと防禦の繰り返しであるため，アタックで破られたときの対策もあらかじめ考えておかなくてはならない．そのひとつが，リニューアルシステムである．これは，何らかの理由でセキュリティメカニズムの一部を交換する必要が生じたときに，それを容易に行えるようにあらかじめ仕組んでおくものである．

実際どのようにリニューアルシステムを組むかは対象により異なるが，暗号システムなどでは幾つか提案がなされている[6]．

●セキュリティポリシー

セキュリティポリシーという言葉を見かけることが多くなっている．ポリシーと言うと，何か大上段に振りかざすように思われるかもしれないが，そうではない．

セキュリティポリシーは，一種の安全対策マニュアル的なもので，何か起きたときにはどうするかということをまとめたものである．中身的には，前々から企業等では実施されていたことである．例えば，暗号の鍵が破られたときにはどのようにすればいいか，コンピュータウィルスが感染した場合はどこにどう連絡し

© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．

てどう対処すべきかと言うようなことである。従って，企業ごとに作らないと，実効あるセキュリティポリシーにならない。

強いて言えば，セキュリティポリシーに対するトップの意識を改革して違反には厳しい処置を取るようになったのが，以前と異なる点かもしれない。

## 5. 暗号の仕組み—SSL を例に

Netscape や Outlook などのインターネットブラウザには暗号・認証機能がついている。これは SSL (Secure Socket Layer) と呼ばれるツールで，証明書を入手すれば誰でも簡単に暗号メールや署名付きメールを送ることができる。

そこでは公開鍵暗号系[1]が基本になっている。公開鍵暗号系では各ユーザが公開鍵と秘密鍵のペアを持っている。公開鍵から秘密鍵が計算できないところがミソである。従って，公開鍵は'公開'できる。この点がそれまでの暗号とは異なる点である。

暗号通信の場合は図1(a)に示すとおり，送信者はメッセージを受信者の公開鍵で暗号変換して送り，受信者は自分の秘密鍵で復号変換する。秘密鍵は受信者しか持っていないので，受信者しか復号できず，メッセージの秘密は保てる。

なお，共通鍵暗号系は，図1(a)の公開鍵と秘密鍵が同一の鍵でどちらも秘密にするものである。公開鍵暗号系が提案される前は全て共通鍵暗号系であった。

一方，署名通信の場合は図1(b)に示すとおり，送信者は自分の秘密鍵でメッセージを署名変換して署名文を作成し，受信者に送る。受信者は送信者の公開鍵でそれを検証する。もし，メッセージが改竄されていたとすると，検証時に引っ掛かることになる。検証は誰でもできるが，署名文は秘密鍵を持っている送信者しか作成できない。

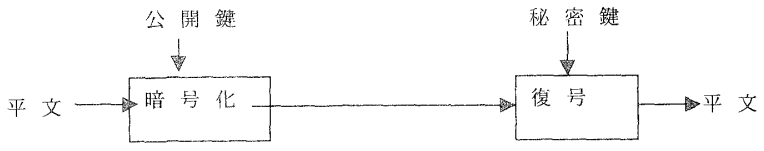
公開鍵暗号系の代表例に RSA がある[5]。一般に公開鍵暗号系は，共通鍵暗号系に比べて処理速度が小さい。

インターネットブラウザには暗号メカニズムはついているが，公開鍵と秘密鍵のペアは鍵発行機関から入手しなければならない。鍵発行機関は現在世界中に沢山あり，有料のケースもあるが，ブラウザの指示に従って適当に選べば，簡単に入手できる。入手した鍵のうち，秘密鍵は自分だけが使うが，公開鍵は他人に渡すので，改竄されてはまずいことになる。そこで，公開鍵は鍵発行機関による署名がついていて，改竄されると検証時に引っ掛かるようになっている。この署名付き公開鍵を証明書という。

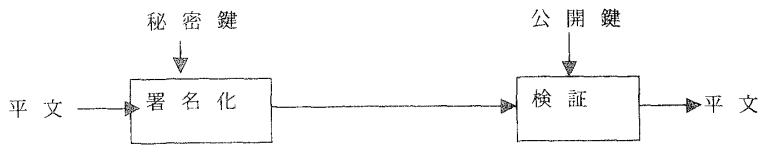
実際に暗号通信を誰かと行おうとすると，相手の公開鍵が必要になるので，証明書を送ってもらわなければならない。あるいは，適当に署名文を送ってもらうと証明書が付いてくるので，それを使えば，暗号化できる。ただし，公開鍵暗号系でメッセージを直接暗号化すると時間がかかるので，実際のメッセージは共通鍵暗号系で行い，そのときのワーク鍵を公開鍵暗号系で暗号化して送っている。

インターネットで銀行振込などを行う場合には，自動的に鍵設定が行われ，ユーザは関知しなくても良いようになっている。単に，ブラウザの錠前マークがロック状態の絵になるだけである。実際にやってみるとわかるが，非常に簡単に暗号通信，署名通信が行えるようになっている。

SSL 他にも SET や SSH などにも公開鍵暗号系は使われている。




(a) 暗号




(b) 署名

図1 公開鍵暗号系


© 日本オペレーションズ・リサーチ学会. 無断複写・複製・転載を禁ず.

SETはクレジットカード決済のためのセキュリティシステムである．最近のスキミングの横行により販売店も信用できなくなりつつあるので，販売店もごまかせないようにする仕組みである．ただ，その分負担も大きくなるため，電子商取引では圧倒的にSSLが用いられている．

SSH（Secure Shell）は，rで始まる遠隔命令を安全にしたものである．今までtelnetはパスワードを回線上に裸で流すために，セキュリティの問題が多かったが，SSHによりパスワードは暗号化されるようになったので，安全度が増している．

## 参考文献


[1] Diffie, W. and Hellman, M. E.: New directions in cryptography, IEEE Trans. on Inform. Theory, Vol. IT-22, No. 6, pp. 644-654, 1976

[2] 遠藤，小出；'コンテンツ配信と不正コピー防止'，電子情報通信学会誌 Vol. 83, No. 2, pp. 117-121, 2000

[3] Mori, R. and Kawahara, M.; 'Superdistribution—The Concept and Architecture', IEICE Trans., Vol. E-73, No. 7, pp. 1133-1146, 1990

[4] Murayama, T., Mambo, M. and E. Okamoto; 'A Tentative Approach to Constructing Tamper-Resistant Software', Proc. of New Security Paradigms '97, 1997

[5] Rivest, R. L., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and publickey cryptosystems, Commun. of the ACM, Vol. 21., No. 2, pp. 120-126, 1978

[6] 栃窪，岡田，遠藤，岡本；'リニューアル認証・暗号システム'，CCS '99 予稿集，pp. 231-236, 1999

[7] 山中，中村，小川，高嶋，曽根原；'著作権保護技術の動向'，情報処理 Vol. 41, No. 4, pp. 382-387, 2000



© 日本オペレーションズ・リサーチ学会．無断複写・複製・転載を禁ず．