道しるべ：暗号と電子社会

岡本 栄司　okamoto@sci.toho-u.ac.jp
東邦大学理学部情報科学科

はじめに

インターネットの広がりと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．これに伴って，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．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，医療機関におけるICカードによる電子カルテなども始まろうとしている．また，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．最近の通産省の調査によると，我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．

インターネットの広がりとITの進展は，さらに社会も変えつつある．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の構図が徐々に浮かび上がってきた．個人が主体になってくると，プライバシーなどを守るため情報セキュリティが不可欠な技術になる．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．今まではクラッカーの個人的な興味による侵入が多かったが，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，政府の取組みにも一段と力が入ってきた．しかし，これと同時に多様な問題や課題も生じつつある．そこで，そのセキュリティ対策の考え方，セキュリティ研究の置かれている状況と今後の研究課題について述べる．

☆　本文には文献3) で発表したものを一部含む．

電子社会の進展と安全性に対する脅威

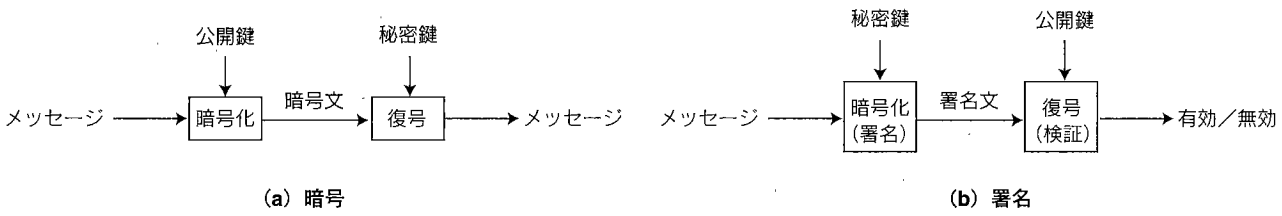
コンピュータが便利になって，家庭にもかなり普及してきている．遠くの人と電子メールで連絡し合ったり，いろいろなホームページを見て買い物をしたり，音楽を楽しんだり，あるいは新しい人との出会いもネットワークを通じて行われているようである．こうなると，もうコンピュータなしでは生きていけなくなる．

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い．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くなる．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始まらない．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持って侵入するが，嵩じると作るほうに回ることもある．

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，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



(a) 暗号　　(b) 署名

図-1　公開鍵暗号系

ユ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，混乱に紛れてそのチェックが終わる前に実行させてしまうものである．

また，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たくさん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，我々ユーザ自身が気を付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くるからである．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．

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2通りある．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み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分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．

なお，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．この意味で，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．万能薬はあり得ず，具体的なアタックごとに薬を調合することになる．

暗号技術と応用例

事前対策の核の1つとして暗号技術がある．ここでは，代表例を用いて，その仕組みを簡単に説明する．

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．したがって，公開鍵は“公開”できる．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，受信者だけが復号でき，メッセージの秘密は保てる．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[2]．一般に公開鍵暗号系は，昔からあるタイプの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たくさんあり，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よ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分かるが，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．

これからの暗号研究

暗号研究は，CryptographyからInformation Security，さらにInformation Managementへと範囲を拡大しつつある．これは，暗号技術の必要性の認識から研究資金の導入が始まり，急速な普及とともに研究者・関係者が増加して研究分野が拡大したことに呼応している．

要素技術の深耕―Cryptography

解読技術の進歩により，新アルゴリズムの開発が進んでいる．共通鍵暗号系[4]，公開鍵暗号系[5]，署名，ハッシュ関数などに加え，量子暗号[6]の新しい暗号も出てきている．セキュリティ特有の現象として，アタックと防止が繰り返されるため，これからも新しいアルゴリズムは出てくるはずである．

暗号技術の実現とともに広がってきた研究―Information Security

電子的な社会への変貌に伴って，多くの取引が電子的に行われ，政府による電子政府への取組みも2003年を目指して始まっている．このカテゴリーに入る研究課題には，侵入検知方式[7]，ソフト保護[8]，著作権保護[9]，セキュリティエージェント[10]，個人識別[11]，ファイアーウォール，ネットワークファイル保護，セキュリティプラットフォーム[12]などがある．これからもやはり課題項目は増え続けるであろう．

一方で，アタック自体の研究もアメリカあたりでは堂々と行われている．テログループや国家ぐるみのアタックの可能性があるからであり，国家防衛の一環と捉えられている．

普及フェーズにおける課題―Information Management

技術だけではカバーできない部分を全体的に守るための課題で，運用管理対策を含む．必ずしも研究向きとはいえないかもしれない．具体的には最近話題となることが多いセキュリティポリシーが中心となる．全般的には，

- 事後対策―ログ，情報保険
- 法制化―罰則
- 国際化―標準化，Global PKI
- 教育，倫理[13]，啓発

などがある．啓発は重要で，情報処理教育の最初の段階で，してはいけないことをしっかり教える必要がある．機会あるごとに指導的な立場の人が情報倫理を説くのは有効であろう．

一般ユーザからみると，暗号に対してかなりの不安感があるように見受けられる．我々は，その不安感を払拭する仕組みを考えなければならない．メッセージは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があるのは当然である．安心して使えるのだということを，確信を持って納得でき，実感できるようにしてあげなくてはならない．

暗号研究環境作り

我々暗号研究に最初からたずさわってきた者にとっては，暗号研究の拡大に伴って，今後さらに研究環境の整備を心がける必要があると考えている．このために，たとえば，電子情報通信学会をはじめとする学会は，研究発表の場などさまざまな方策を提供してきた．

今後は，国際化進展が重要になり，日本から出てまずアジア，次に世界の仲間入りをしていくことになろう．現在，日本が始めて世界に広がりつつある国際会議シリーズとして，Asiacrypt，ISW（Information Security Workshop），PKC（Public Key Cryptography）がある．特にAsiacryptは今年からIACR（International Association of Cryptology Research）主催となって，Crypto，Eurocryptと並び称されることとなった．参加して討論に加われば，有用な情報が得られよう．

また，これらの国際会議で発表した研究成果は，国際的なジャーナルに正論文として載せて初めて一人前となるものである．現に権威あるジャーナルは多いが，来年度から発行されるIJIS（International Journal of Information Security）[14]もこうした目的のために作られたものである．

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) Rivest, R. L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126 (1978).
3) 通信・放送機構:「情報通信セキュリティ技術に関する研究開発」プロジェクト成果発表会予稿集, pp.156-158 (2000).
4) http://csrc.nist.gov/encryption/aes/
5) 岡本, 藤崎, 内山, 森田: 公開鍵暗号「EPOC」および「PSEC」, 電子情報通信学会情報セキュリティ研究技術報告予稿集 (May 2000).
6) http://osogami.virtualave.net/
7) http://www.vogue.is.uec.ac.jp/%7Ezetaka/Public/kenkyu/anzen/papers/intro_ids.html
8) Murayama, T., Mambo, M. and Okamoto, E.: A Tentative Approach to Constructing Tamper-Resistant Software, Proc. of New Security Paradigms'97 (Sep. 1997).
9) 小野: いま, 注目される技術―電子透かし, Cyber Security Management, Vol.1, No.9, pp.114-121 (2000).
10) Kitazawa, S., Okamoto, E. and Mambo, M.: Secure Access Control Agent for Distributed Files, JWIS'98 (Dec. 1998).
11) 菅 編: ここまできたバイオメトリックスによる本人認証システム, 情報処理, Vol.40, No.11, pp.1071-1103 (Nov. 2000).
12) Nam, S., Okamoto, E., Shinoda, Y. and Mambo, M.: A Design and Implementation of a Platform for Self-Deciphering Secret Communication, Proc. of 1996 IEEE Int'l Symp. on Information Theory and Its Applications, pp.242-245 (1996).
13) 越智, 土屋, 水谷編: 情報倫理学, ナカニシヤ出版 (2000).
14) http://link.springer.de/link/service/journals/10207/index.htm

(平成12年9月12日受付)