暗号リテラシー

Cryptography Literacy

澤田秀樹
山形大学基盤教育院
Hideki SAWADA
Institute of Arts and Sciences, Yamagata University, Yamagata 990-8560

要約
本稿は著者の山形大学における基盤教育としての情報リテラシー，大学院理工学研究科における暗号理論の教育・研究を通して得られた，インターネットと情報端末を安全に使いこなすために必要な最小限度の暗号の基礎知識，すなわち暗号リテラシーの在り方を提案するものである．
キーワード：情報リテラシー，暗号，NP 問題，通信プロトコル

1　序

山形大学における教養教育は，平成22年度(2010年度)から学士課程教育における基盤教育として，その内容を発展・整理して「導入科目」「基幹科目」「教養科目」「共通科目」「展開科目」で構成することとなった．既に平成８年度から独自のテキスト[1]を使用して全学的に実施されていた情報処理は「情報リテラシー」として，『学問の実践に役立つ知識や能力，あるいはそれを根底で支える健康な体力を身に付けさせることを目的とする』共通科目のなかで，引き続き全学生を対象に開講されている．

情報リテラシー教育のための情報処理テキストは，前半がパソコンの扱いやメールの送受信，文書作成等の一般的な内容，後半はセキュリティや著作権，UNIX や通信プロトコルといった発展的な内容からなっている．大学入学前における情報処理教育が浸透しつつあるのか，未だにパソコンに不慣れな学生がいるにも拘らず，新入生の平均的なパソコン習熟度は年を追って向上している．テキスト前半の一般的な部分は山形大学情報処理システム利用上の注意や固有の問題の周知にとどめ，いずれ情報処理教育の力点は後半のセキュリティや著作権問題，通信プロトコルの解説に移っていくだろう．

情報セキュリティと著作権問題に共通する技術の１つは暗号であり，それはインターネットを流れる情報の盗聴や，著作物の改竄を防ぎ，更に本人を確認するために必要不可欠なものといえる．

本稿はインターネットと情報端末を安全に使いこなすために必要な最小限度の暗号の基礎知識，すなわち暗号の役割とその安全性の根拠，および通信プロトコルとの関係を，暗号リテラシーとして提案するものである．

2　暗号とは

情報セキュリティシステムの要素の１つで，情報の交換や記憶集積に際して，第三者にそれが知られること，あるいはさらに当事者をも含めて故意による情報の改変を防ぐため，その対象となる情報を秘匿する技術や方法のことである．[2]

ネットショッピングを例に，暗号の役割を考えよう．

1. **ユーザ名とパスワード**でパソコンにログオンする．
   このパスワードは**暗号化**されてパソコンに保存されている．第三者がそのパソコンを自由に操作できる状況になければ，パスワードの解除は出来ない．しかし簡単に推測されるパスワードを使用していたり，キー入力を盗聴するソフトがインストールされている場合は，暗号の強度とは関係なく情報セキュリティは保てない．

2. アドレスを確認してから，ショッピングサイトを開く．
   有名サイトと一文字違いといった，詐欺サイトがあるので注意が必要となる．

3. 商品を選択する．

4. 個人情報を入力する．既に会員である場合はショッピングサイトの**ユーザ名とパスワード**を入力する．

   遅くともこの段階からは，ショッピングサイトと交わされる情報は **https**, Hypertext Transfer Protocol Security というプロトコル(通信手順)により**暗号化**されて送受信されていなければならない．通常のプロトコル **http**, Hypertext Transfer Protocol では，サイトから送られる情報や入力する情報は暗号化されていないので，簡単に盗聴することができる．ブラウザのアドレスが https に変わらない場合は，作業を中断すべきである．

5. 決済方法を選択する．

6. 場合によってはクレジットカードの番号を入力する．

7. ショッピングサイトからの注文確認メールを受信する．

8. 選択した決済方法に従い商品を受け取る．

これらの一連の操作がすべて連携して滞りなく実行されて，初めて安全に買い物が出来ることになる．ネットショッピングに限らず，セキュリティシステムにおいては環のようにつながった様々な要素のどれもが等しく重要で，その一箇所でも破綻すればシステムは安全ではなくなる．教養として理解しておくべきことは，まさにこの環としてのセキュリティシステムと，各要素の安全性に関する知識である．

セキュリティシステムの環のなかで，一番弱い要素は**人**である．パスワードを設定しない，簡単なパスワードを設定する，他人とパスワードを共有する，使用中のパソコンの画面をロックせずに席を離れる，ホームルータを初期設定のまま使用する，良く考えずに個人情報を入力してしまうなどである．一方一番強い要素は**暗号**である．暗号は鍵を総当りで試して解読するといった方法では，コンピュータの能力を越えてしまうため，解くことが出来ないことが数学的に「保証」されている問題を使用して，作られている．

コンピュータの能力を越えるとは何かを説明しよう．

3　NP 問題とは

本人確認を伴う電子マネーやインターネットオークションなどには公開鍵暗号が，データの秘匿には対称鍵暗号が使用される．

この対称鍵暗号は古来から使用されている暗号化と復号化を対称的に１つの鍵で実行するもので，電子的に金庫を実現したものといえる．この場合重要なのは候補となる鍵の総数で，攻撃側がコンピュータを駆使して総当りで順に調べても，彼らが生きてる間にはとても終了しないような，膨大な鍵の総数 2^{128} から 2^{256} を持つように設計されている．ここで注意しなければいけないのは，この安全性はあくまで攻撃側の計算能力に対して相対的に定まる点である．現に 1977 年に米国商務省標準局によって米国連邦政府機関の標準として公開された DES 暗号 (Data Encryption Standard)※ は既に次世代暗号標準 AES(Advanced Encryption Standard)† に替わられている．

本人確認を伴う場合は公開鍵暗号が使用される．この暗号を使用するためには，一人一人に公開鍵と秘密鍵という２つの異なる鍵を分配する必要がある．

互いに面識がない Alice と Bob でも公開鍵のリストを共有し，公開鍵と秘密鍵を組み合わせれば，通信の秘密を守りしかも互いに相手を確認することができる．このアイデアは 1976 年に W.Diffie と M.Hellman が提唱したが，その仕組みは書留郵便を例にとると分かりやすい [3]．秘密鍵を Alice と Bob が持つ自分の印鑑ないしサインとし，公開鍵はそれぞれの住所とする．Alice が Bob に現金を送るとしよう．Alice は専用の封筒を用意し，現金を入れて封印しサインする．このサインは Alice にしか出来ないので Alice の秘密鍵といえる．次に公開鍵リストに対応する住所録から見つけた Bob の住所を記入し，郵便局で登録し Bob に発送する．書留は Bob の住所に配達され，その住人のサイン (Bob の秘密鍵) を確認の上，手渡される．一方 Bob は Alice のサインと住所から書留の発信元の確認ができる．

この方式の重要な点は，当事者の一人一人が互いに異なる１組の鍵つまり公開鍵と秘密鍵の組を持っていれば，誰とでも安全に通信出来るところにある．対称鍵暗号では玄関の鍵のような開閉両用の鍵を１つ使用するだけなので，Alice は事前に別の安全な経路で Bob にその鍵を渡しておかねばならない．しかも同じ鍵は別の相手には使えないから通信相手が変る度に新たな鍵を用意することになり，外交や軍事といった関係者が少数な場合を除いては，膨大な鍵が必要となるので対称鍵暗号で本人確認を実現するのは現実的ではない．

ではどうすれば秘密鍵 (閉じる鍵) と公開鍵 (開ける鍵) の組が作れるのだろうか？　それにはコンピュータが苦手とする数学の問題，例えば素因数分解を利用する．整数 32353319 を素因数分解すれば 32353319 ＝ 5683×5693 となるが，筆算で短時間に 32353319 が２つの素数 5683 と 5693 の積になることを見つけるのは極めて困難である．これは現在使われているコンピュータにとっても同様で，一般には整数が大きくなるほどスーパーコンピュータを駆使しても因数分解は困難になる．つまり現在使用されているコンピュータにはまだその構造に適した効率の良い素因数分解アルゴリズムが見つかっていない．

素因数分解問題は，素因数の発見は困難であるがその一方見つかった素因数の積が元の整数に等しくなるかを検算するのは容易である，という特徴を持っている．このような特徴を持つ問題を NP(Nondeterministic Polynomial time) 問題，非決定性多項式時間問題という．NP 問題には NP 完全とよばれる，任意の NP 問題の解決をその問題に帰着できるような，問題の集合がある．例えば

※標準的な DES の鍵の総数は 2^{56} である．

† 2000 年 10 月 2 日に選定された．

ナップザック問題：
「入力：自然数の列 $\{S,M_1,M_2,...,M_n\}$
決定すること :0,1 を要素とする列 $\{b_1,b_2,...,b_n\}$ で

$$S=b_1M_1+b_2M_2+\cdots+b_nM_n$$

となるものが存在するか？」
は NP 完全問題である．このような NP 完全問題が１問でも入力データの大きさ x に対してその多項式 x,x^2,x^3 …時間でコンピュータが解くことができればすべての NP 問題は効率よく解けてしまい，公開鍵暗号の安全性の根拠は失われる．しかしその一方で NP 完全問題は現在使われているコンピュータでは効率よく解くことはできないと予想されている．

４　プロトコルとは

インターネット上の通信は，標準化された規約に基づいて行われる．この規約をプロトコル（通信手順）とよぶ．もともとプロトコルとは外交上の儀礼を指す言葉であり，面接試験の挨拶や自己紹介，電話の好ましい応対法も一種のプロトコルといえる．

ホームページの閲覧には http が，電子メールの送信には **smtp**(Simple Mail Transfer Protocol) が使用され，さらにそれらはTCP/IP(Transmission Control Protocol /Internet Protocol) というプロトコルに支えられている．「支えられている」という言い回しにはプロトコルの階層的な構造が反映している．電話をかける手順も同様に階層的である．つまり電話線や無線の基地局という物理的な基盤の上でデータに変換された音声を送り，マナーにのっとって相互に相手を確認して要件を伝えるのは階層的といえる．

OSI の階層	TCP/IP の階層
アプリケーション	アプリケーション (http や smtp)
プレゼンテーション	
セッション	
トランスポート	トランスポート
ネットワーク	ネットワーク (IP)
データリンク	データリンク（イーサネットなど）
物理	物理（ケーブルの配線）

TCP/IP は国際標準化機構 ,ISO(International Organization for Standization) が定めた 7 階層からなる OSI(Open Systems Interconnection) 参照モデルに対比し上の表のように５階層から構成される．詳しくは参考文献 [3] などを参照されたい．

ホームページを閲覧したりメールを交換する場合はこの TCP/IP に基づいて情報が送受信される．接続を確立するために端末 A とサーバ B 間で３回，接続要求 ($A \rightarrow B$)，接続許可と接続要求 ($B \rightarrow A$)，接続許可 ($A \rightarrow B$)，と相互にデータを交換するという特徴がある．この特徴からわかるようにホームページを閲覧したりメールを交換することは双方向の通信となる．つまりホームページの閲覧はアナログテレビやラジオの受信とは異なり，接続を確立したときには受信者の情報はホームページのサーバ側にも送信される．

暗号を使う場合，上の５つの階層のどの部分が暗号化されるかを意識する必要がある．再び電話を例にとれば，通信回線が暗号化されていれば盗聴の危険はかなり低くなるものの，防音設備のない部屋で受話器を取れば少なくともどちらか一方の話は他人にも聞かれる可能性が高くなる．互いに防音室から暗号化回線を使って通話すれば，当事者が通話内容を他人に洩らさない限り安全である．

５　まとめ

以上がインターネットにおける暗号の役割であり，暗号リテラシーとしての最小限度の基礎知識である．セキュリティシステムは情報と組織，組織と人，人と端末，端末とネットワークを結ぶ環として理解すべきで，各要素のもっとも弱い部分が，システム全体の弱点となる．しかし情報を安全かつ快適に扱うことはトレードオフの関係でもあるので，業務の目的に合わせてどこまでセキュリティを徹底するかは，その時々の関係者の政治的な判断といえる．

暗号を本格的に勉強するには数学専攻の学部生レベルの群や有限体，整数論，確率のほかに計算量理論や量子力学の知識も必要となる．日常的にサーバやネットワークを管理して情報セキュリティの現場を知っておくことは，理論と応用のバランスを保つ上でとても好ましい．

参考文献

[1] 山形大学情報処理教育実施会議編．2010『情報処理テキスト』山形大学

[2] 澤田秀樹．2005『暗号理論と代数学（第４版）』海文堂．

[3] 澤田秀樹．2002『暗号と代数プログラミング（第２版）』海文堂．

[4] 澤田秀樹．2009『Linux 情報戦略』海文堂．