情報セキュリティ歳時記 13

安全な暗号

前川　徹
早稲田大学 国際情報通信研究センター

➲ 共通鍵暗号と公開鍵暗号

現在利用されている暗号は，大きく2種類に分けられる．共通鍵暗号と公開鍵暗号である．

共通鍵暗号は暗号化と復号に同じ鍵を用いる暗号である．2000年以上の歴史があり，1970年代に公開鍵暗号が考え出されるまで暗号といえば共通鍵暗号のことであった．共通鍵暗号は，暗号化と復号の処理時間が比較的短くて済むという利点はあるが，取引や機密情報の伝達に利用する場合には，暗号化する側と復号する側で同じ鍵を持っている必要があるため，鍵をどのようにして他人に知られないようにして相手に送るのかが問題になる．また，関係者が多くなるにつれて暗号鍵の管理が大変になる．機密保護のために情報を交換する相手ごとに別の鍵を使う場合，情報交換相手の数だけ鍵を管理しなければならない．

一方，公開鍵暗号は暗号化と復号に異なる鍵を用いる．暗号化に使った鍵では復号できない．代表的な公開鍵暗号であるRSA暗号の場合，鍵は一対になっており，どちらか一方で暗号化すると，もう一方でないと復号できない．したがってどちらか一方を公開し（これを公開鍵と呼ぶ），もう一方を他人に知られないように管理する（これを秘密鍵と呼ぶ）．Aさんに情報を暗号化して送りたい場合は，一般に公開されているAさんの公開鍵で暗号化して送ればよい．誰かが盗聴などの手段によって暗号文を不正に入手しても，Aさんの秘密鍵がなければ復号はできない．したがって，この方法だと情報を交換する相手がどれだけ増えても自ら管理する鍵は1つでよくなるし，相手に鍵をどうして送るかという問題も解決できる．

さらに公開鍵暗号を使って，ネットワーク上で相手が本人であることの確認と情報が改ざんされていないことの証明が可能になる．これがディジタル署名である．

➲ ディジタル署名の方法

前述したように，RSA暗号の鍵は一対になっており，どちらか一方で鍵を閉めればもう一方でないと開けられない．Aさんの公開鍵で暗号化したものは，Aさんの秘密鍵でないと復号できないし，その逆に，Aさんの秘密鍵で処理したものは，Aさんの公開鍵でないと元に戻らないのである．つまり，Aさんの公開鍵で復元できるメッセージはAさんの秘密鍵で処理したものであり，Aさんが自分の秘密鍵をきちんと管理しているという前提に立てば，そのメッセージはAさんから送られてきたものだということになる．これがディジタル署名の仕組みである．

図は，1995年にABA（American Bar Association）が公認したディジタル署名付きの暗号通信を行う方法である．ディジタル署名は，送りたいメッセージをハッシュ関数によって要約したデータを使って行われる．ディジタル署名処理された要約をAさんの公開鍵で処理し，復号化した本文を自分で要約したものと比較することによって，メッセージがAさんからのものであり，かつメッセージが改ざんされていないことも確認できる．また，メッセージが第三者に盗み読まれるという心配もない．

なお，このABA公認の方法では本文も公開鍵暗号によって暗号化しているが，公開鍵暗号は共通鍵暗号に比べて処理時間がかかるため，本文を共通鍵暗号で暗号化してその共通鍵を公開鍵暗号で暗号化して送る方が一般的である．

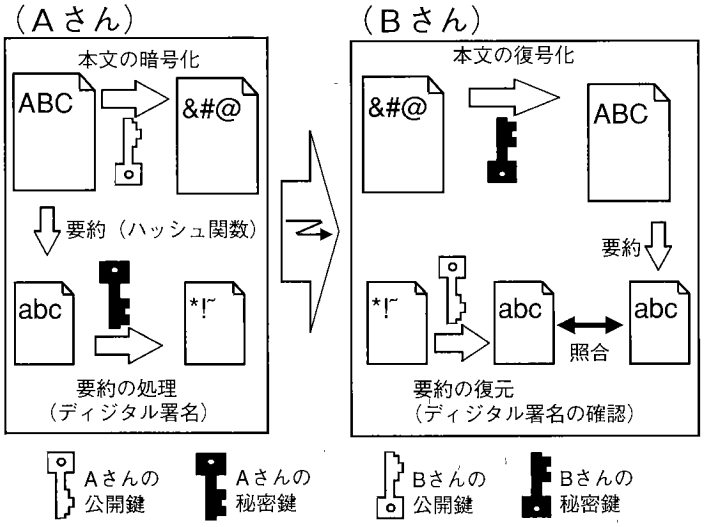
さて，残された問題は，Aさんの公開鍵であると思っている鍵が，本当にAさんの公開鍵であるかどうかであるが，これを保証してくれるのが認証局であり，PKI（Public Key Infrastructure）である（認証局とPKIの仕組みについては省略する）．

➲ 暗号の強度

さて，これで暗号を利用して安全に情報が送れるだろうか．答えはノーである．ここまでの話は，正当な鍵を持っていなければ暗号文を平文に戻せないという前提で進めてきた．しかし，歴史を見れば，数多くの暗号が解読されてきている．前々号で紹介したように，第2次世界大戦中にドイツ軍が用いていたEnigmaも，日本が1930年代終わりから1945年まで利用していた外交用暗号（米国がPurpleと名付けた暗号）も，DVDビデオの暗号も解読されている．また，1970年代に米国連邦政府が標準暗号として採用したDESも1999年1月にわずか22時間15分で解読されたことは先月紹介したとおりである．

暗号は解読されてしまっては何の役にも立たない．

ABA公認のディジタル署名付き暗号通信の方法



したがって，まず安全な暗号方式を選択する必要がある．つまり，解読が困難な暗号である．解読の難しさをここでは暗号の強度という．そして，一般的に暗号の強度はアルゴリズムと鍵の長さで決定される．

鍵の長さが暗号強度の決定要因であることは分かりやすい．容易に想像できるように，より多くの鍵から利用する鍵を選べた方が安全である．選択できる鍵の数が100個と100兆個では，100兆個の選択の余地がある方が解読は難しくなる．鍵の種類が100個なら100回試せば必ず解読できるからだ．コンピュータ処理される暗号の鍵は，0と1のビット列で表現できるので，このビット列の長さを鍵の長さといい，一般的には鍵が長い方がより安全だということになる．つまり，鍵の長さが3ビットしかなければ，鍵は8種類しかないが，128ビットであればおよそ3.4×10の38乗という膨大な数の鍵から選ぶことができる．

仮に，鍵長が自由に選べる共通鍵暗号で，鍵長がDESと同じ56ビットの場合，22時間で解読可能だと仮定すると，鍵長を40ビットにすると1.2秒で解読でき，128ビットにすると10の19乗年以上の時間が必要だという計算になる．いかに鍵長が重要であるかが理解できるだろう．

しかし，鍵長がいくら長くても，暗号アルゴリズムに欠陥があれば安全な暗号とはいえない．暗号アルゴリズムの設計者が気付かない欠陥が発見され，解読時間が短縮できることが発見されたケースも少なくない．現在，米国連邦政府が次世代の暗号標準（AES）を選定中であるが，この過程でもアルゴリズムの欠陥が見つかって候補から削除された暗号があるという．

アルゴリズムの欠陥は，鍵の長さより深刻な問題である．DESが22時間15分で解読されたとはいえ，それは特定の鍵が破られただけで，別の鍵を利用している暗号を解読するためには，また22時間あまりの時間を要する．しかしアルゴリズムの欠陥は，鍵をどう選ぼうが欠陥なのである．

アルゴリズムは公開が原則

では，いっそのことアルゴリズムを公開しなければよいのではないか．アルゴリズムを公開しなければ，欠陥を発見されることもないだろうし，解読の手がかりも少なくなり，暗号はより安全になるだろう．そう考える人もあるかもしれない．現実にも，アルゴリズムを公開していない暗号も数多く存在する．しかし，これはきわめて危険な選択である．もし仮に，非公開のアルゴリズムに欠陥があり，誰かが偶然に簡単な解読方法を発見した場合，大変なことになる．その暗号を利用しているシステムがすべて脅威に晒されることになるのである．ニコラス・バランは『情報スーパーハイウェイの衝撃』の中で，あるハッカーが米連邦政府が普及させようとしたEESという暗号アルゴリズムの欠陥を発見して簡単に暗号を解読してしまうという架空のエピソードを書き，アルゴリズムが公開されていない暗号の危険性を指摘している．

もちろん，公開されている暗号アルゴリズムでも，ある日突然欠陥が発見される可能性はある．しかし，公開されている暗号アルゴリズムの場合，多くの暗号研究者によって安全性がチェックされており，非公開のアルゴリズムに比べて，暗号の安全性を脅かすような欠陥が発見される可能性は小さいと考えられる．非公開のアルゴリズムは，不特定多数の研究者のレビューを受けていないだけに，その点が不安なのである．

したがって，安全な暗号の条件の1つは，アルゴリズムが公開されていて，世界中の暗号研究者によって十分研究され，その時点で欠陥が指摘されていないことなのである．新しい暗号を開発した企業が，いくら安全性を訴えても，インターネット上で暗号解読コンテストを実施したという実績を示しても，それは十分とはいえない．特に社会的に重要な情報システムに用いる暗号については，こうした点を踏まえて慎重に選ぶ必要がある．

今月の参考文献等
1) 辻井重男著：暗号 ポストモダンの情報セキュリティ，講談社選書メチエ73 (1996)．
2) ニコラス・バラン著（勝又美智雄訳）：情報スーパーハイウェイの衝撃，日本経済新聞社 (1994)．

（平成12年2月15日受付）