column

●本当のインターネットをめざして

vol.27

公開鍵暗号系？

太田 昌孝

東京工業大学 情報理工学研究科

mohta@necom830.hpcl.titech.ac.jp

共有鍵暗号系と公開鍵暗号系

古典的な暗号系は，通信の双方が秘密を共有し，それを利用して通信内容への署名や秘匿を行う共有鍵暗号系である．

これに対して，現代の公開鍵暗号系は，だれにでも公開された公開鍵とそれに対応する秘密鍵の組を利用する．通信内容を暗号化するのに公開鍵を利用し，解読に秘密鍵を利用すれば，秘匿通信が行える．通信内容への署名に秘密鍵を利用し，署名の確認に公開鍵を利用すれば，認証された通信が可能となる．公開鍵暗号が成立するためには，そのような用途に利用可能な秘密鍵と公開鍵の組のうち，公開鍵から秘密鍵を計算することが計算量的に事実上不可能なものが存在すればよい．大きな整数の積や有限体上での指数は比較的簡単に計算できるが，現在まで知られている方法では大きな整数の素因数分解や大きな有限体上での離散対数問題は計算が困難である．これらの性質を公開鍵暗号として利用したのが，それぞれRSA暗号系とE! Gamal暗号系である．

共有鍵暗号系では通信する相手ごとに異なる共有鍵を用意しなければならないので，N対Nの通信にはN^2個の鍵が必要である．これに対して公開鍵暗号系では，通信相手全員に同じ公開鍵を配布すればいいので，鍵の数はNで済む．そこで，暗号の専門家によると，情報通信網が発展して暗号が大規模に利用される時代には，公開鍵暗号系しかスケールしないとなる．

しかし，公開鍵暗号の利用状況をみると，この議論がおかしいことが分かる．公開鍵暗号系は計算が遅いので，通信の最初や要所要所で共有鍵を交換するために使い，実際の通信には共有鍵暗号を使う．つまり，共有鍵の数はN^2どころではない．

開かれた環境で見知らぬ他人と鍵をあらかじめ共有しておくことは不可能だが，同様に，見知らぬ他人の公開鍵を知っておくことも不可能である．公開鍵暗号系では，他人の公開鍵が認証されている必要がある．第三者が偽造した他人の公開鍵を使ってしまうと，第三者の署名を真正なものと判断したり，秘匿したはずの情報を第三者に解読されてしまうからだ．

そこで，公開鍵暗号系では認証局というものを置く．認証局は，その公開鍵を広く周知しておく．各人はあらかじめ自分の公開鍵を認証局に登録し，自分の公開鍵に認証局の署名を付加した証明書をもらっておく．すると，通信相手がその認証局を信用し，その認証局の公開鍵を知っていれば，自分の公開鍵を認証してもらえる．認証局の階層や認証局どうしの相互認証を通じて世界中の認証局を関連づけておけば，自分と通信相手が同じ認証局を利用していなくてもよい．

共有鍵暗号系でも，鍵配布局というものを設置すれば同様のことが行える．各人はあらかじめ鍵配布局と鍵配布用の鍵を共有しておく．通信相手も同じ鍵配布局と（別の）鍵配布用の鍵を共有していれば，鍵配布局を通じて個々の通信のための共有鍵を交換できる．鍵配布局の階層や鍵配布局どうしの相互認証も公開鍵暗号系同様に可能である．

認証局も鍵配布局も，運用の手間は同程度である．

通信の節約？

共有鍵暗号系と公開鍵暗号系との大きな違いは，通信量にある．共有鍵暗号系では，通信のための鍵交換のたびに鍵配布局と通信しなければならないが，公開鍵暗号系では，一度認証局に証明書をもらえば以後認証局との通信は不要である．

これは一見公開鍵暗号系の利点のように思える．しかし，インターネットの時代には，通信は事実上無料であ

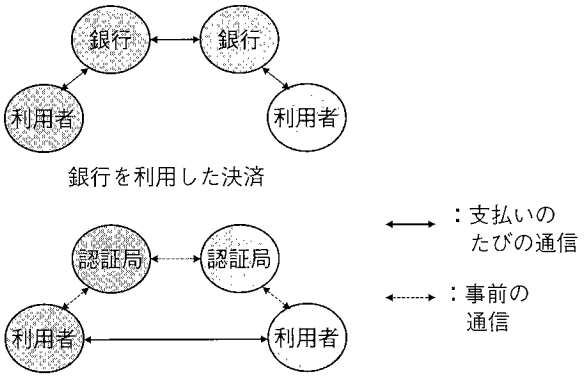

図-1　電子決済の様子

る．インターネットは常時接続が当然であるし，無線インターネットが普及すればどこでも事実上無料の通信が利用できる．鍵配布局のサーバはインターネットの各所に複数個配置すれば，事実上ダウンすることはない．自分の側のインターネットが断線している場合には，鍵配布局と通信できないが，そもそもの通信相手とも通信できないのだ．インターネットにより情報通信網が発展して暗号が大規模に利用される時代には，共有鍵暗号系で十分である．

ここで，通信が高価だという固定観念があると，ついつい「同じ相手と再び通信するときのために，鍵を安全に秘匿しておくのが難しい」などと考えがちだが，鍵など通信のたびに作り直せばいいのだ．

そもそも，公開鍵暗号の実運用においては，認証局と頻繁に通信する必要がある．証明書には有効期限があるが，再認証の手間を減らすため期限は長めに設定してある．すると，期限の途中で証明書を失効させる必要が生じる．そこで，認証局は失効した証明書名のリストを自らの秘密鍵で証明した証明書失効リストというものを短い間隔と有効期限で発行している．通信に際しては，受信者は有効期限内の証明書失効リストを入手せねばならず（送信者が入手して通信とともに送ってもいい），認証局との通信は必須である．

公開鍵暗号系の欠陥

公開鍵暗号系の本質的欠陥は，署名に際して認証局との通信が必要ないことにある．

通信による電子決済を考えてみよう．分散システムでは通信の遅れや誤りは不可避であるため，ある事象を正確に1回発生させることは不可能で，たかだか1回か，少なくとも1回，という保証しかできない．通信では通常，上位層で再送して「少なくとも1回」を保証する．電子メールが届かないのは困るが，2回届くぶんには問題ないからだ．しかし，電子決済では不払いも二重払いも論外である．そこで，そのような不正を行わないと信用のおける第三者を決済に介在させる必要がある．これが，為替取引における銀行の役割である．銀行と顧客は信頼関係に基づき鍵を共有する（図-1）．問題が発生した場合，銀行が顧客に賠償責任を負うこともある．銀行は顧客に対して「信用」というコンテンツを供給しているのだ．その代価として決済金額に応じた手数料が徴収されるのも当然である．

これに対して，認証局は電子決済の双方の身元を抽象的に確認するだけである．決済は認証局との通信なしに行われ，認証局は内容に関知できない．当事者どうしが直接取引きすると，確かに決済のたびの手数料は不要だが，逆に，問題が発生してもどこにも責任の持っていきようがない．こんな決済システムは使いものにならない．見知った相手との通信にすら当然のように認証局が介在してしまうのも問題である．公開鍵暗号系と電子マネーにより銀行の役割は低下し認証局に置き換わるという話がまことしやかに説かれてきたが，幻想にすぎない．

契約に対する電子公証にしても同様で，契約者双方の身元が抽象的に保証されても印鑑登録と同程度の意味しかなく，証明すべきは契約の内容自体である．契約内容を公証人に保証してもらうには，契約の当事者全員が公証人とそれぞれ共有した鍵で署名した契約書を公証人に送ればいい．

公開鍵暗号系による抽象的な保証も秘匿には使えるが，これまで何の関係もなかった相手との通信内容を秘匿しても，意味はない．

暗号の専門家にとっては暗号技術が自己目的化しがちだが，社会にとって暗号は信用というコンテンツを流通させる技術にすぎず，存在しない信用を作り出すものではない．信用とは2者の間の社会的かかわりをもとに生まれるものであり，その際に共有鍵を発生させれば必要にして十分である．

何も難しく考えることはない．キャッシュカードの暗証番号も銀行との共有鍵なのだ．

（平成13年5月15日受付）