PKIとは？

内海章博[†]

キーワード：PKI，公開鍵暗号方式，認証局，証明書

1. PKIの背景

インターネットがビジネス分野でも急速に進化し、インターネット上での商品売買やオンラインバンキングなどのインフラとして使われるようになるに伴い、個人情報やクレジットカード番号等の漏洩の危険性が利用者に認知されており、いかにセキュリティを保ち、通信の安全性を確保するのが大きな課題になっている。

一般的に、インターネットに潜む危険例として、「なりすまし」、「盗聴」、「改ざん」、「否認」の4点がとり挙げられている。

「なりすまし」とは、インターネットで、あなたが今アクセスしているサイトが本当のX社のサイトなのか、X社を語ったまったく別の第三者が立てたサイトなのかを確認する術がないことが挙げられる。コピー可能なデジタルコンテンツの世界では、ホームページ自体は誰でも簡単に作成でき、インターネット上になりすましたサイトを立てることも、技術的に不可能ではない。

次に、「盗聴」とは、正しいサイトにアクセスしていたとしても、そのサイトとの通信は、誰にでも盗み読まれてしまう危険を意味する。通常インターネットでは、通信内容は平文のまま流れ、ネットワーク上の不特定のサーバを経由して受け渡されるため、ネットワークの途中でデータを取込み、内容を盗

み読むことは技術的には難しいことではない。

さらに、「改ざん」とは、ネットワークの途中で通信内容を別のものに入れ替えることが技術的には可能であるため、見ているウェブサイトの掲載情報、途中で何物かに書き換えられてないかどうかを確認する術がないことを意味する。ウェブサイトの掲載情報により重要な決断を下さなければならぬような場合、その情報自体の信頼性の確保は非常に重要となる。

「否認」は、「改ざん」や「なりすまし」と大きな関係を持っている。例えば、自分が行った取引行為を、「第三者が私になりすまして行った」と言い張ったり、実は10個の注文をしたのに、「注文したのは1個であり、誰かが改ざんして「0」を一つ付け加えた」と主張したりして、自分の行った契約を否定し

てしまうというものである。

「改ざん」、「なりすまし」の可能性が存在する以上、こういった主張に真向から反論することが非常に難しくなってしまう。ウェブサイトが単なる個人的な趣味としての用途であった頃には、これらは特に大きな問題となることはなかったが、Eコマースの利用が広まるとともに、利用者の安全性の確保は欠くことのできない要件となった。実世界では対面し、契約を取り交わすことで回避できていたリスクが、インターネット上では歴然と存在してしまうのである。

2. PKIとは？

このようなインターネットの危険性を回避し、安全な通信を行うためのセキュリティインフラが、PKI (Public Key Infrastructure) である。

[†]株式会社東京放送 開発局 デジタル開発センター
"What is PKI" by Akihiro Uchimi (Technology Development Center for Digital Media Development, Tokyo Broadcasting System, inc., Tokyo)

図2 共通鍵暗号方式

図3 電子署名

PKIは、主にメッセージ等を暗号化および復号するための「鍵」と、鍵の正当性を保証する「証明書」、証明書を発行する「認証局」から構成される。

■ 公開鍵暗号方式

PKIでは公開鍵暗号方式という暗号技術を使用する。

公開鍵暗号方式とは、共通鍵暗号方式の欠点を解消するものとして考案されたもので、暗号化と復号で異なる二つの鍵を使用する方法である(図1)。

この方式では、キーペアと呼ばれる一対の鍵が生成され、一方の鍵を使っ

て暗号化したものは、対となるもう一方の鍵を使用しなければ復号できない。この一対の鍵は「秘密鍵」と「公開鍵」と呼ばれている。

公開鍵とは、文字どおり「外部に公開する鍵」で、メッセージを暗号化するときを使う。逆に秘密鍵は、公開鍵で暗号化されたメッセージを復号する唯一の鍵であるため、他人に盗まれないよう厳重に管理しなければならない。

図1のように、AがBにメッセージを送信する場合で考えてみると、Bが自

分宛てのメッセージを暗号化して欲しい場合には、Aにあらかじめ自分の公開鍵を渡しておき、その公開鍵でメッセージを暗号化して送ってもらえばよいことになる。暗号化されたメッセージを復号化できるのは自分(=B)の秘密鍵だけであるため、他人にメッセージを読まれる心配はない。

逆に、Aに暗号化したメッセージを送りたい場合には、あらかじめAの公開鍵を入手しておき、その公開鍵を使って送りたいメッセージを暗号化することになる。

このように自分の公開鍵を広く配布することによって、多くの人が暗号化されたメッセージを自分宛てに送ることができるようになる。逆に秘密鍵は、他人の手に渡ってしまうと自分宛ての暗号化メッセージを解読されてしまうので、誰にも盗まれないよう厳重な管理が必要である。

一方、共通鍵暗号方式では、暗号化するための鍵と復号するための鍵に同じものを使用する(図2)。この方式の場合、メッセージを暗号化した鍵は、復号する際にも必要となる(同じ鍵を使う=共通鍵)ので、通信を行う相手の数と同数の鍵を準備し、保管しなくてはならないことが欠点となっていた。

一方、公開鍵暗号方式では、メッセージを交わす相手が何人になろうと、自分の秘密鍵だけ持っていればいいのである。公開鍵暗号方式は、最初に述べたリスクのうち「盗聴」を防ぐのに有効な手段である。

公開鍵暗号のもう一つの使い方は、あるデータが本当に発信者からのものである、途中で改ざんされていないことを証明することである。これを電子署名という。電子署名は、先ほど紹介したデータの暗号化とは逆で、署名をした人が自分の秘密鍵を使って行う。電子署名の仕組みを図3に示す。図3のように、AがBにメッセージを送る場合には、メッセージ(明文)と一緒に、自分の秘密鍵で暗号化したメッセージと一緒に送る。この二つのメッセージを

図4 証明書のフォーマット

図5 証明書の検証プロセス

受け取ったBは、まず暗号化されたメッセージをAの公開鍵で復号し、それと平文のメッセージを比較する。これが一致した場合、「メッセージは改ざんされていない」ことになる。なぜならば、Bがメッセージを「公開鍵を用いて復号できる」ということは、「Aだけが持つ秘密鍵で暗号化された」メッセージであるから、「暗号化したのはAである」ということが言えるからである。秘密鍵を持っているのは、鍵ペアの所有者本人(=A)だけなので、電子署名が正しく検証できれば、メッセージは間違いなく発信者から送られたものであり、途中で改ざんされていないことが証明できる。この方法によれば、「なりすまし」や「改ざん」だけでなく、「否認」のリスクも回避することができる。

3. 証明書について

■ 証明書の必要性

暗号化通信を行う場合や電子署名を検証する際に、相手の公開鍵が必要である。公開鍵はどのような方法で配布してもよく、誰が所有していてもよいものであるため、どうやって安全に相手の公開鍵を入手すればよいのかという疑問が残る。

例えば、誰かが偽の公開鍵をあなたの公開鍵だと偽って配布した場合、送

られた暗号化メッセージを自分の秘密鍵で復号することができなくなる。さらに、暗号化してあなたに宛てたメッセージを他人が読めることになってしまう。

そこで今度は、自分の公開鍵を正しく配布するための証明書、つまり、「公開鍵証明書」というものが必要になる。公開鍵証明書は、第三者があなたの公開鍵を「本物」だと証明してくれるものである。相手の公開鍵を受け取ったならば(通常、証明書の中に公開鍵が含まれる)、証明書の内容に不備がないか確認することで、公開鍵の所有者が確かに本人であると検証できるのである。

■ 証明書の内容

公開鍵証明書の中には、公開鍵そのものに加えて、公開鍵の所有者情報/公開鍵を証明する認証局情報/証明書の有効期間/認証局の電子署名、などが含まれている。

証明書は印鑑証明に例えられることがあるが、その内容も印鑑証明と似通っている。例えるなら、「公開鍵」は登録された印鑑で、「認証局」は印鑑証明を行ってくれる市役所や区役所と言える。

証明書のフォーマットは、ITU-Tが定めたX.509という規格に沿ったものが広く使用されており、X.509の証明

書フォーマットには、主に図4のような情報が格納されている。

図5に、Aの公開鍵証明書を受け取ったBが、Aの公開鍵証明書の正しさを検証する過程を示す。

Aから公開鍵証明書を受け取ったBは、公開鍵証明書を発行した認証局の電子署名を検証することによって、証明書に記載されている公開鍵が本物であるかを確かめることができる。Bが予め持っている認証局の公開鍵証明書が正しいものであるとわかっていれば、その公開鍵証明書を使って電子署名を検証し、Aの公開鍵証明書が正しいものであるかどうか判断することができる。

4. 認証局について

■ 認証局の役割

公開鍵流通に「証明書」が必要なことはおわかりいただけたと思う。

この証明を行ってくれる第三者機関のことを、認証局(Certification Authority: CA)と呼ぶ。現在、いくつかの商用認証局がすでに存在しており、主として地域住民を対象とした非営利の認証局も立ちあがっている。

AとBが暗号通信を行う場合、証明書の内容に不備がないか検証するが、その際、同時に証明書を発行した認証局が、信頼できる認証局かも確認する。

AとBの双方が信頼できる認証局からの証明書であることが確認できた時点で、Aが受け取った公開鍵が本当にBのものであることが証明されるのである。

では、AとBが「認証局を信頼する」とはどういうことなのであろうか？例えば、CがBに成りすまして、ある認証局から、Bの証明書を取得することが可能ならば、AもBもその認証局を信頼できない。このようなことを避けるため、認証局には、証明書を使用するユーザからの信頼性を担保するために遵守すべきガイドラインが必要となる。

このようなガイドラインには、認証局の鍵が盗まれ、勝手に証明書が発行されてしまったり、悪意の第三者に証明書を発行してしまったり、証明書の発行記録が改ざんされたり、といったことを避けるために、秘密鍵の管理や十分な本人確認の必要性、オペレーションルームへの厳重な入退室管理など、数多くの要件が記述されている。また、認証局の運用方針は、認証局運用規程(CPS: Certificate Practice Statement)として公開されている。これは、認証局を利用する人が、認証局の信頼性を判断するためのものである。

■ 認証局の証明書

それでは、受け取った証明書が偽の認証局から発行されていた場合、どうしたらよいのか？

そのためには、認証局を証明するための証明書が必要となってくる(また証明書が必要なの？といった感じであるが)。その証明書を用いて認証局の署名を検証する。

認証局が自身の存在を証明するための証明書は、その認証局が自分で発行する場合と、上位の認証局が発行する場合がある。図6のように、認証局が階層構造を取っていて、各認証局が親となる上位の認証局から証明書を発行

してもらう場合があるが、その場合も遡って行くと、自分で自分の証明書を発行できる認証局が存在する。この最上位の認証局を「ルート認証局」といい、発行する証明書を「ルート認証局証明書」という。

ルート認証局の証明書には、他の認証局の署名ではなく、認証局自身の署名、つまり、「自己署名(Self-Sign)」がなされている。

■ ルート認証局

図6のように、AがX認証局、BがY認証局という、それぞれ二つの認証局から証明書を発行され、二つの認証局は、同じルート認証局(=Z認証局)から証明書を発行されているとする。この場合も、AもBも相手の証明書を発行している認証局を知らないため、信頼関係は築けないことになる。しかし、ここでAとBとの間に「Z認証局を信頼する」という事前了解があれば、例えば、AとBがXやYという中間認証局を知らなくとも、ルート認証局を元にした信頼関係が成り立つのである。AがBから証明書(+公開鍵)を受け取った場合、Aは次のように検証を行う。

まず、AはBの証明書と一緒にY認証局の証明書を受け取ることが必要である(この時点で、AもBも「Z認証局」というルート認証局を信用している)。そして、Aは、受け取ったY認証局の証明書が自分の信頼するルート認証局(=Z認証局)から発行されていることを、Y認証局の証明書の署名で確認する。次にAは、受け取ったBの証明書が確かにY認証局から発行されたものであることを、Bの証明書に付いている署名を検証して確認するのである。

5. む す び

2003年末より開始される地上波デジタル放送では、テレビ受信機にモデムやLANポートなど、インターネットアクセス機能が実装される予定である。地上デジタルテレビジョン放送事業者

図6 ルート認証局と階層構造

運用規定「TR-B14(1.1版)」では、TCP/IPやHTTP1.1(RFC2616)のサポートや、セキュリティ機能としてのTLS(Transport Layer Security) 1.0/SSL(Secure Sockets Layer) 3.0の実装、データ放送のリソースとしてのルート証明書の伝送など、通信機能が拡張され、認証やセキュリティに関する規定が追加されている。

これにより、テレビを使用したオンラインショッピングやバンキングなど、Tコマースと呼ばれる商取引アプリケーションが利用可能となる。このことは、文中で述べたインターネットのリスクにパソコンだけでなく、テレビも晒される時代がやってくる可能性があることを示唆している。

最後に、本稿が読者の方々のPKIや認証への理解の助けに少しでもなれば幸いである。(2002年12月24日受付)

うちのあきひろ
内海 章博

1990年、東北大学大学院電子工学専攻修士課程修了。同年、キヤノン(株)入社。通信技術関連の開発に従事。1997年、(株)東京放送に入社。同技術局にて、衛星伝送関連の設備構築ならびに運用業務を経て、2001年より、開発局デジタル開発センターにて、データ放送、サーバ型放送、ブロードバンド関連業務に従事。