名古屋大学技術職員研修を受講して　-電子証明書の基礎-

○池田将典、加藤俊之、柘植朗、谷口泰広

名古屋大学全学技術センター　共通基盤技術支援室　情報通信技術系

概要

我々は、昨年9月に行われた平成19年度名古屋大学技術職員研修情報通信コース「Webサーバ認証とAjax入門」を受講した。今回はこの研修で学んだ、PKI(Public Key Infrastructure)公開鍵暗号技術を利用した電子証明書を中心とした社会基盤の、その基礎知識と有用性について紹介する。

1　はじめに

高性能で簡単に操作できるPC、携帯電話の普及、安価なブロードバンド回線による常時接続環境の整備などが、インターネット利用の普及に拍車をかけ、今やネットの活用は、経済活動に密着したものとなりつつある。しかし、現実の世界よりも高いとされる匿名性により弊害も生まれている。たとえば、送信元を偽って配信されるフィッシング詐欺メールや、正規ユーザになりすました不正アクセスなどは、ネットの匿名性を悪用した犯罪である。これらの脅威に対し、SSL, S/MIME, 電子認証技術, 電子証明書などを組み合わせる事により、契約書への捺印や、銀行口座の開設、確定申告といった作業も、ネット越しでも行えるようになって来ている。電子証明書とは、これまではネットの匿名性により、実現が困難だったサービスをも提供できるようにする技術と言える。今回は名古屋大学技術職員研修で学んだ電子証明書の基本的仕組みについて紹介する。

2　なぜ電子証明が必要か

先に述べたように、近年「盗聴」,「改竄」,「なりすまし」,「事後否認」といった脅威がより身近な問題となって来ている。これらを個別に見ていくと以下のような事が明らかとなってくる。

- 盗聴：電子商取引においては企業のデータや取引データなど、他人に知られては困るものが飛び交うことになる。これらのデータを不正な利用者に盗まれる危険性がある。また、重要な電子メールを盗み見られる危険性もある。　盗聴の危険性に対する有効な対策は、ネットワーク上に流れるデータを暗号化する事となる。
- 改竄：電子データはデジタル情報であるため、紙に書いた文字とは違い、容易に内容を書き換えることが出来うる。このため、悪意を持ったユーザによって情報が不正に改竄される可能性がある。データ内の数字を一桁改竄されるだけでも甚大な被害が発生しうる。改竄の危険性への対策は、電子データのメッセージ認証を行う事や、デジタル署名を施す事となる。
- なりすまし：ネットワーク上では相手が見えないため、第三者が当事者になりすまして不正な行為を行う可能性がある。電子メールにおいて、差出人の名前を詐称したり、正規ユーザの認証情報を盗聴し、その認証情報を利用するといった行為が見られる。なりすましの危険性への対策は、強固な認証方法の導入や、電子メールにデジタル署名を付加する事となる。

•事後否認：改竄, 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行為を、「第三者が私に成り済まして行ったものだ」と言い張ったり、 実は 10000 個の注文を出していたのに、「注文したのは 1000 個であり、誰かがデータを改竄して “0”を１つ付け加えたのだ」と主張したりして、自分の行った行為を否定してしまうというものである。改竄, なりすましの可能性が存在する以上、こういった主張に反論することは非常に難しくなる。事後否認への対策は、当事者の認証と電子署名により否認出来ない環境を作る事となる。

これら脅威を取り除く方法には様々な種類が考えられるが、PKI を利用すれば、これらの危険性を包括的に除去することが出来る。

3　ＰＫＩとは

PKI とは、Public Key Infrastructure の略であり、「公開鍵基盤」あるいは「公開鍵暗号基盤」と訳される。

PKI は電子証明書や認証局、公開鍵暗号方式などを用いて、盗聴・なりすまし・改竄・事後否認といった危険性から身を守るための仕組み全体を指す。つまり、PKI とは、誰もが意識せずに使用できるインフラ技術を表している。

PKI とは「公開鍵」暗号方式という技術を利用した、セキュリティの「基盤」である。

4　ＰＫＩ技術要素

4.1　共通鍵暗号方式 (Symmetric cryptography)

暗号化する鍵と復号する鍵に同じ鍵を用いる暗号方式。暗号文の送信者と受信者で同じ鍵を共有する必要があるため、共通鍵暗号（対照鍵暗号）と呼ばれる。送信者と受信者の間でそれぞれの鍵を秘密に管理する必要がある事から、秘密鍵暗号とも呼ばれる。

共通鍵暗号方式の長所は、「処理が比較的高速である」という点である。もちろん、共通鍵暗号方式のアルゴリズムには幾つも有る為、各アルゴリズム間で比較すると差異はある。しかし、次に述べる公開鍵暗号方式と比べれば総じて高速であると言えるため、大量のデータの暗号化に向いている。

逆に短所となるのは、「鍵の配送・管理に気を使わなければならない」という点である。共通鍵暗号方式の仕組みを利用するには、受信者があらかじめ鍵を入手しておく必要がある。暗号化したデータ自体は、盗聴されても鍵がなければ解読される可能性は非常に低いため、暗号化したデータをメールに添付してネット経由で相手に送っても一定の安全性は確保出来る。しかし、受信者が暗号鍵を知らない場合は復号は不可能となる。

そこで、暗号化の無い平文のメールを送り、その中に「鍵は 123456」などと記述したとする。このとき、伝送経路上で悪意のある第三者が盗聴を行っていたら、この鍵で暗号化したデータは全て悪意のある第三者に筒抜けとなってしまう。

また、大勢で相互に共通鍵暗号方式を利用してデータをやり取りする場合、鍵の数が増え、管理が非常に面倒な物となる事も短所の一つである。

代表的な共通鍵暗号方式のアルゴリズム

•DES：Data Encryption Standard の略。1970 年代に米 IBM が開発し、1977 年に米国標準の暗号方式として採用された。最近はコンピュータの処理性能の増大などにより安全性が低下したため、徐々に使われ

なくなってきている。鍵の長さは56bit。

•Triple-DES：DESのアルゴリズムを暗号化→復号→暗号化と鍵を変えて3回繰り返すことにより 、DESよりも強固な暗号化として使われている。1回目と3回目に同じ鍵を使用する2KEY方式と、3回とも異なる鍵を使用する3KEY方式がある。鍵の長さは112bit、または168bit。

•IDEA：International Data Encryption Algorithmの略。PGP(Pretty Good Privacy)というメールなどの暗号化を行うアプリケーションに使われている暗号アルゴリズム。1992年にスイスのAscom-Tech社によって開発。鍵の長さは128bit。

•AES：Advanced Encryption Standardの略。米国国立標準技術研究所（NIST）が、より高速で強い共通鍵暗号方式を公募し、さまざまな候補の中から選ばれた暗号方式。DESの後継の次世代暗号標準。無線LANデータの暗号化（WPA2）などに使われている。鍵の長さは、128bit、192bit、256bit。

4.2 公開鍵暗号方式 (Public Key Cryptography)

公開鍵暗号方式は「公開鍵」と「秘密鍵」という二つの鍵を使って暗号化や復号を行う。公開鍵と秘密鍵は二つで一組のペアになっており、一方の鍵で暗号化した平文は、ペアのもう一方の鍵を使わないと復号できないという関係になっている。この性質を用いることで、ネットワーク上の離れた相手に安全に情報を送信出来る

公開鍵暗号方式と呼ばれる理由は、この二つの鍵のうち一方をだれでも利用できるように公開するため。こちらの鍵を「公開鍵」と呼ぶ。もう一方の鍵はユーザー本人だけが秘密に保管することから「秘密鍵」と呼ばれる。

公開鍵暗号方式は共通鍵暗号方式と比較して、鍵を受け渡しする必要がないのが最大の利点となる。暗号化に使用する公開鍵は、インターネット等公開先から誰でも入手できるので、鍵の安全な配布を可能とした。また、共通鍵のもうひとつの問題点であった鍵の管理も容易となる。共通鍵の例と同様に四人で互いに通信を秘密に行いたい場合でも、管理しなければならない鍵は自身の秘密鍵一つのみとなる。たとえ誰か一人の鍵が漏洩した場合でも、他の人物には影響しない。

公開鍵暗号方式では暗号化, 復号の処理に要する時間は、共通鍵暗号方式と比較して数百倍以上の時間を必要とする。そのため実際には、高速な処理を可能とするため、公開鍵暗号方式と共通鍵暗号方式を組み合わせて使用する。

メッセージを送信する際に、一時的に使用する共通鍵（セッション鍵）を作成し、メッセージ全体を暗号化そして、共通鍵を受信者の公開鍵暗号方式の公開鍵を用いて暗号化し、メッセージと一緒に送信する。受信者は、まず暗号化された共通鍵を自分の秘密鍵で復号した後、メッセージ全体の平文を得る。

代表的な公開鍵暗号方式のアルゴリズム

•RSA：開発者であるRivest, Shamir, Adleman ３名の頭文字をとって命名。現在最も広く使われている公開鍵暗号方式。素因数分解の数学的な難しさに基づく暗号方式。

•DSS：Digital Signature Standardの略。米国国立標準技術研究所（NIST）が1991年に提唱したデジタル署名のためのアルゴリズム。離散対数問題の数学的な難しさに基づいている。

•ECC：Elliptic Curve Cryptosystem 楕円曲線暗号とも呼ばれる。離散対数問題に楕円曲線を用い、RSAの1/6程度の鍵長で同程度の強度があると言われている。

•DH：Diffie-Hellman 1976年に発表された世界で初めての公開鍵暗号のアルゴリズム。共通鍵を安全に交換するための鍵配送アルゴリズム。

4.3 ハッシュ関数

ハッシュ関数は、入力データから固定長のビット列を出力する関数であり、出力されたハッシュ値から元の値を算出する事は出来ない。元のデータの一部を変更するとハッシュ値が大きく異なるという性質がある。

デジタルデータは、文章であろうと画像であろうと、全てのデータは 0 と 1 との組み合わせで表現される。つまり、どんなデータであっても、一つの数値とみなすことが出来る。ハッシュ値とは、ある数値をハッシュ関数と呼ばれる関数で演算した結果である。ハッシュ値は元のデータ長に関わらず、128bit 程度の一定の長さとなる。hash という言葉の通り、元のデータをアルゴリズムに従って細かく切り刻んで、一定の長さに整えたものと言える。

代表的なハッシュ関数のアルゴリズム

- MD4：128bit のハッシュ値を生成する。MD5, SHA-1 などの源流。1991 年に脆弱性が実証され、2004 年には、ハッシュ衝突を作成する事が可能である事が報告された。
- MD5：1991 年に開発された MD5 は、前身である MD4 の安全性を向上させたものである。広く用いられているハッシュ関数で、任意長メッセージから 128bit のハッシュ値を生成する。1996 年に衝突攻撃によって部分的に弱点が存在することが判明している。2007 年 4 月 IPA は MD5 の脆弱性について警告した。これは電気通信大学の太田和夫教授（暗号理論）の研究グループが発見したもので、MD5 ハッシュから理論的に元のパスワードを求めることが出来たというものである。この対策として MD5 を用いる APOP ではなく SSL の利用を推奨している。
- SHA-1：アルゴリズムは MD4 を元にしており、MD5 よりも攻撃に対して強いと考えられている。2007 年現在、SHA は生成するビット長が異なる SHA-1 (160 ビット)、SHA-224、SHA-256、SHA-384、SHA-512 の 5 種類が存在している。

4.4 電子署名

メッセージを作成した本人であるか、内容が改竄されていないかを検証する技術を電子署名と呼ぶ。

元のメッセージに対しハッシュ関数と公開鍵暗号を用いることにより、改竄の検出が可能となる。これをデジタル署名(Digital Signature)と呼ぶ。

デジタル署名を用いると、以下のことが確認できる。

- 署名を作成した者が本人である事（本人認証）
- メッセージが改竄されていない事（完全性）

デジタル署名を作成することは署名(Sign)と呼び、デジタル署名の有効性を確認する事を署名の検証(Verify)と呼ぶ。

注意しなければならない点は、デジタル署名では内容の暗号化はしないという事である。メッセージ自体は平文なので盗聴は可能となる。

デジタル署名の仕組みを用いることによって享受できる利点に「否認防止」という効果もある。電子署名を行った場合、署名出来るのは本人だけである事から、署名した事を後から否定することは不可能となる。

5　ＰＫＩ

PKI(Public Key Infrastructure)とは、公開鍵暗号技術を用いた電子証明書を中心とした社会基盤である。PKI では、公開鍵の所有者を第三者信用機関(TTP: Trusted Third Party)に保障してもらう。TTP は公開鍵の所有者を何らかの方法で確認し、公開鍵とその所有者を保障する電子証明書を発行する。電子証明書は、公開鍵と所有者の情報が記載された上で、TTP が署名を行う。この証明書を発行する機関の事を、証明局(CA: Certification Authority)という。

5.1　ＰＫＩの構成要素

PKI は証明書を作成, 保管, 配布, 破棄を行うために機関, 人, ハードウェア, ソフトウェア, 処理, 手続きで構成される。主な構成要素は以下の通りである。

- 認証局 (CA: Certification Authority)：公開鍵に対し認証局の秘密鍵で署名を行うことにより、公開鍵と秘密鍵の所有者を結びつける、公開鍵証明書を発行する。認証局にはルート認証局(root CA)と中間認証局(intermediate CA)がある。ルート認証局は上位の認証局による認証を受けず、自分の正当性を自ら証明する。他の認証局に対してデジタル証明書を発行し、認証局に対する信頼の拠り所となる。ルート証明書の信頼性は、厳しい監査を受けることや、認証業務運用規程(CPS)を公開すること、運用実績や知名度など、デジタル証明書以外の方法で示される。ルート認証局以外の認証局が中間認証局で、ルート認証局など上位の認証局からデジタル証明書を発行してもらうことで、自らの正当性を証明する。
- 登録局(RA: Registration Authority)：PKI を大規模で運用するた際に、証明書発行の機能の一部を認証局から分離して請け負う。証明書申請を受け取った際に、本人性の確認を行い、CA に対して証明書の発行や執行を要求する。
- リポジトリ (Repository) ：証明書および証明書失効リスト(CRL: Certificate Revocation List)を PKI 利用者へ公開する。

5.2　認証局の重要性

公開鍵証明書の信頼の基盤となる証明局は、正しく運用される必要がある。そのため、認証局のセキュリティがどうなっているのかを利用者に提示する認証局運用規定(CPS: Certification Practice Statement)を規定する。また、公開鍵証明書の利用, 目的に関する規制, 範囲を証明書ポリシー(CP: Certification Policy)として規定する

認証局が絶対に防がなければならないのは、認証局の秘密鍵の漏洩である。万が一漏洩した場合は、不正に証明書が発行されるだけではなく、認証局も含めて PKI システム全ての証明書の再発行が必要となる。

5.3　CRL (Certificate Revocation List)

証明書には有効期限が在るが、有効期限内でも証明書が利用できなくなる場合がある。秘密鍵の紛失, 漏洩した場合。証明書の所有資格を失った場合。証明書の記載内容に変更があった場合である。このような場合は、証明書は認証局により破棄手続きが行われ、失効する。認証局は定期的に CRL を発行し、利用者に公開する。

5.4 X.509 証明書

公開鍵証明書の標準として、ISO/IEC の国際標準として規定された X.509 がある。この仕組みにより、公開鍵の所有者を認証局が証明する事が出来る。電子証明書には、公開鍵だけでなく、証明書として機能するのに必要な情報が含まれている。証明書の有効期限を含めて認証局が署名を行っているので、証明書を受け取った者が有効期間が過ぎていないか確認する事が出来る。

WebPage が SSL を用いて表示されている場合、X.509 証明書がクライアント PC へ送付されている。この X.509 証明書に署名を行っている発行者の X.509 証明書は、あらかじめブラウザにインポートされている事で、クライアント PC 側で署名を検証出来る。署名が正しければ、WebPage の証明書に対し、内容の改竄が無い事、その認証局によって発行された事が確認できる。

6 ＰＫＩアプリケーション

6.1 SSL (Secure Sockets Layer)

SSL は、クライアント／サーバ間における安全な通信環境を提供するプロトコルである。SSL は、証明書を利用することにより、通信の守秘性, 認証. 完全性を確保する。SSL は、TCP/IP レイヤ上で動作し、様々なアプリケーションプロトコル (HTTP, LDAP, FTP, TELNET 等) で利用出来る。

SSL を利用するには、サーバとクライアントに証明書が必要になるが、クライアントを認証せず、サーバのみの認証とする場合は、クライアント側の証明書は必要無い。

SSL は、以下のセキュリティ機能を提供する。

- 認証 (Authentication)：X.509 証明書を利用する事により、サーバ及びクライアントの認証を行い、第三者によるなりすましを防ぐ。クライアントの認証はオプションとなっており、サーバのみの認証とする事も可能。
- 守秘性 (Confidentiality)：サーバとクライアント間の通信を暗号化する事により、第三者への情報の漏洩を防ぐ。暗号化は共通鍵(RC5, トリプル DES など)によって行われる。共通鍵をサーバとクライアント間で交換するために、X.509 証明書に含まれる公開鍵(RSA, DH など)が用いられる。
- 完全性 (Integrity)：サーバとクライアント間で交換されるデータの完全性を確認し、情報の改竄を防ぐ。完全性の確認にはメッセージ認証コード(MAC: Message Authentication Code)を用いる。

SSL は、Web (HTTP) において最もよく利用されている。SSL の主な利用目的を以下に示す。

- 通信の暗号化と完全性の保証：サーバとクライアントの通信を暗号化することにより、クレジットカード番号や個人情報などの重要な情報をネットワークの盗聴から保護する。暗号化と同時に改竄の検出を行うため、通信内容（データ）の完全性も保たれる。
- サーバの認証：Web における電子商取引(EC)を利用する際には、利用者はアクセスする Web サーバが本当に信頼できるかを確認する必要がある。ドメインは誰でも取得出来るため、URL に含まれるドメイン名は必ずしも信用の根拠とはならない。SSL を利用する事により、アクセスしている Web サーバを証明書によって認証する事が出来る。
- クライアント認証：Web サーバにアクセスするクライアントに対して、証明書を利用した認証を要求する事が出来る。従来利用されている ID とパスワードによる認証よりも、強固な認証が実現出来る。

6.2 S/MIME (Secure/Multipurpose Internet Mail Extension)

S/MIME は、証明書を利用して電子メールに暗号化とデジタル署名のセキュリティを提供する。S/MIME は、既存の技術である MIME を利用しているため、既存のメールサーバ(MTA)で問題なく動作する。S/MIME は、電子メールに限らず、MIME を扱える他のプロトコル(HTTP など)でも利用することが出来る。

S/MIME を利用すると、メールの暗号化(暗号メール)とデジタル署名の付与(署名メール)が実現出来る。また、証明書の送付にも利用出来る。暗号メールにおいては、送信者は受信者の証明書を使ってメールを暗号化し、受信者は自分の秘密鍵でメールを復号する。署名メールでは、送信者は自分の秘密鍵でメールに署名をつけ、受信者は送信者の証明書で署名の検証を行う。署名メールは、通常では送信者はメールに自分の証明書を付与する形で送信する。

S/MIME は、以下のセキュリティ機能を提供する。

- 認証 (Authentication)：X.509 証明書とデジタル署名を利用し、メールの送信者とメッセージの認証を行う。
- 守秘性 (Confidentiality)：メールを暗号化して送信することで、第三者への情報の漏洩を防ぐ。暗号化には送信者が生成した共通鍵を使用する。
- 否認防止 (Non Repudiation)：X.509 証明書を用いたデジタル署名により、送信者がメールを送信した事実を否認する事を防止する。
- 完全性（Integrity）：X.509 証明書を用いたデジタル署名により、添付ファイルを含むメール本文の内容が、送信時と相違ない事が確認出来る。

7 認証局の運用組織

7.1 大手認証機関

Netcraft の調査結果では、VeriSign が認証局市場のシェア 70%以上を占め、以下 Comodo, Go Daddy などが続く。2006 年の Verisign による GeoTrust 買収以降は、商業市場はほぼ寡占状態に近づいている。商用認証局はサーバ証明書の年間利用料が最低 8 万円代からと、けっして安くは無い。

対して、無料サービスによる証明書の場合、ルート証明書が往々にしてブラウザに組み込まれていない等の本質的な問題が有る。

7.2 政府認証基盤 (GPKI: Governmental PKI)

日本政府の「電子政府」構想に基づく認証基盤。行政側の認証基盤として各省庁が運営する府省認証局と、それらをつなぐ総務省のブリッジ認証局が、商業登記認証局や民間認証局と、相互に認証することにより、申請書などに付加されるデジタル署名の有効性を担保する。外国政府の認証局や地方自治体の運営する認証局とも必要に応じて相互認証が行なわれる。霞ヶ関 WAN の認証基盤である。

7.3 地方公共団体組織認証基盤 (LGPKI: Local GPKI)

地方公共団体が住民, 企業等との間で実施する申請, 届出等の手続き、あるいは地方公共団体間の文書のや

り取りを電子的に行う。総合行政ネットワーク(LGWAN)の認証基盤であり、ブリッジ認証局を介して GPKI と相互認証を行っている。

7.4　公的個人認証サービス (JPKI)

住民基本台帳に記録されている国民に対して電子証明書を発行する認証基盤で、インターネットを使った申請が申請者本人からであることを電子的に確認するサービス。申請, 届出といった行政手続きのオンライン化を実現する。

現在は住民基本台帳カードを介してのみ利用可能。GPKI, LGPKI と相互認証を行っている。

7.5　全国大学共同電子認証基盤 (UPKI: University PKI)

大学間連携のための認証基盤。SINET に加入している大学等に参加資格があり、無料でサーバ証明書の発行を受けられる。ただし、発行されるサーバ証明書の有効期限は 2009 年 3 月末までとなっている。

8　終わりに

ここまで先の研修で学んだ PKI の仕組みを紹介してきた。それまでは漠然としか知らなかった、電子証明書について理解を深める事ができ非常に有意義な研修だった。

今後は、学校内外への公式な連絡や発表の際は、PKI を利用した証明が増えていくものと予想される。暗号化，証明書の技術は一層重要なものとなって行く事は間違いない。

より理解を深めるため今後とも学んでいきたい。

参考文献・資料・URL

[1]　相戸 浩志「よくわかる最新情報セキュリティの基本と仕組み 増補改訂版―基礎から学ぶセキュリティリテラシー」秀和システム, ISBN-10: 4798015881, ISBN-13: 978-4798015880

[2]　平野 靖「PKI の基礎とその可能性」平成 19 年度名古屋大学技術研修テキスト

[3]　内藤 久資「ネットワーク社会における電子認証の重要性」平成 19 年度名古屋大学技術研修テキスト

[4]　大川 敏生「SSL について」平成 19 年度名古屋大学技術研修テキスト

[5]　日本ベリサイン株式会社 電子証明書と PKI 入門　http://www.verisign.co.jp/basic/pki/

[6]　独立行政法人 情報処理推進機構 PKI 関連技術解説　http://www.ipa.go.jp/security/pki/

[7]　日経 BP 社 Itpro PKI の仕組み　http://itpro.nikkeibp.co.jp/article/lecture/20070419/268962/

[8]　日経 BP 社 Itpro 情報セキュリティ入門　http://itpro.nikkeibp.co.jp/article/COLUMN/20060214/229302/

[9]　米国ベリサイン・インクによる米国ジオトラストインク買収についてのお知らせ
http://www.verisign.co.jp/press/2006/pr_20060518.html

[10]　Netcraft SSL Survey　http://news.netcraft.com/archives/2007/10/26/netcraft_ssl_survey.html

[11]　高木浩光@自宅の日記 - 「UPKI イニシアティブ」でサーバ証明書発行プロジェクト
http://takagi-hiromitsu.jp/diary/20071202.html