# デジタル世界の身分証明証その２
# ー情報基盤センターPKI プロジェクトー

## 1.はじめに

前回の記事(Vol.6, http://www.itc.u-tokyo.ac.jp/DigitalLife/Vol6/Digital_Life_Vol.6.pdf)で佐藤周行助教授がPKIの概要を説明しました。今回からは「PKIって何？」ということを少しくだけた感じで説明しようと思います。

くだけた感じで説明するとは書きましたが、話の展開上、どうしても技術的なことも説明しなければなりません。読んで分からない場合は適当に流してくださって結構です。とりあえず、「フ～ン」と理解した気になって読み続けていただき、PKI に親しんでいただけましたら幸いです。

なお、分かりやすく書くため多少、正確でない表現もあると思いますがご了承ください。

## 2.PKI（ピーケーアイ, Public Key Infrastructure）って何？

最初だけちょっと技術的な話を書かせてください。PKIとは直訳すると「公開鍵（暗号）基盤」と訳されますが、簡単にいうと、1.インターネット上での様々な脅威（盗聴、なりすまし、改ざん、事後否認）を防ぐ技術基盤（インフラ）の総称であり、また、セキュリティに関するだけでなく、2.様々な電算システム（人事･給与関係、財務関係、学務関係、研究協力関係、学生の成績閲覧等）に権限のある人だけが安全にログイン（認証）するために利用されます。

PKIの利用の目的を大別すると次の3つになると言われています。

1)認証
- 電子証明書というデジタル世界（インターネット上）の身分証明書により、ログイン（認証）した人の身分保障をします
- なりすましの防止…偽造不可能な電子署名（実社会いう印鑑やサイン）により、確かに本人ということを証明します

2)完全性
- 改ざんの防止…改ざんされた場合、改ざんされたことがわかります
- 事後否認の防止…偽造不可能な電子署名（実社会いう印鑑やサイン）を文書等に付与することによって、作成者に対して否認させません

3)秘匿性
- 盗聴の防止…データを暗号化して解読できないようにします

ところでPKIでつまずく理由としては「PKIとは一言でいうと○○です」といったものがないため戸惑ってしまうからです。私も様々な人からPKIの話を聞く毎に違う技術のことを言われ、「で、結局は何なの？」と理解するのに非常に苦労しました。

しかし、ある時思ったことは「PKIとはいろいろな技術の『総称』ではないか？」と。確かにそう思ったら、今までの話がようやく「点から線」となり、理解することができました。つまり「暗号もPKI」「電子署名もPKI」「公開鍵、秘密鍵もPKI」なのです。

なお、公開鍵と秘密鍵の説明については長くなりますし、一言では書けませんので、次回以降に譲ります。興味のある方はyahooやgoogleなどで検索してみてください。

## 3. PKI って世の中ではこんなことで利用されています

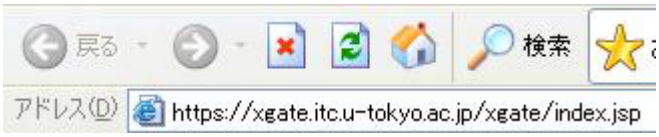
上記の内容はちょっと技術的な説明で興味を削がれたかもしれません。恐らくどういう場面で PKI を利用するかイメージが湧きづらいと思います。

そもそもみなさんにとって「PKI ってどんな場面で使っているの？」「研究者だけの世界で自分には関係ないよ」と疑問に思われる方も多いでしょう。でも実はみなさん、無意識に PKI を利用しています。「エッ？いつ？」とビックリされたかもしれません。

たとえば、オンラインショッピングやインターネットバンキングを利用するとき、自分の名前や住所、クレジットカード情報などを入力します。そのときアドレスバーを見ると、いつも見る「http://～」ではなく「https://～」と表示されていることに気付いたことはありますか？（図１）その状態で実は無意識に PKI の技術を利用しているのです。この「https://～」となってからのデータのやり取りは、すべて暗号化されているので、第三者から盗聴されることはありません。図２の例はインターネット・エクスプローラー（バージョン 6.0）ですが、画面の右下に南京錠のようなマークがあると思います。（図２）　その南京錠みたいなものをダブルクリックしてみてください。次に図３のようなウィンドウが開いたら、全般というタブをクリックしてみてください。そこに「誰が（発行者）」「誰を（発行先）」といったことを証明しています。これをサーバ証明といいます。（図３）　このサーバ（≒ホームページ）がドメインの中で正式に運用されていれば、安心して個人情報を送信することができます。

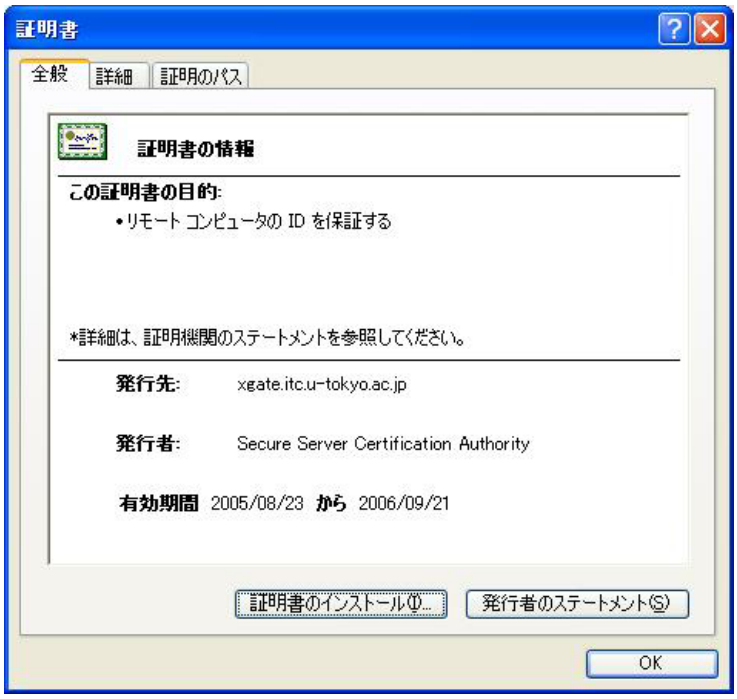
なお、「誰が（発行者）」証明するというのが重要で、みなさんが信頼できない（または知らない）人（または会社）から「このサーバ（≒ホームページ）は信頼できますよ」と言われても何も意味はないと思います。この「誰が（発行者）」がという話は長くなりますので、残念ながら次回以降に譲ります。

最近、マスコミを賑わしている「フィッシング詐欺」は、悪意のある者が利用者から個人情報を得る（釣る）ために、本物とソックリのホームページを作成します。そのためたとえば、インターネットバンキングの利用者は、見た目は本物とソックリなため自分が利用している銀行と思い込み、口座番号や暗証番号を入力して送信してしまいます。当然サーバ証明の無い（または、聞いたことのない所からサーバ証明書を得た）偽のホームページなので、悪意のある者に個人情報を知られてしまうのです。



（図１）

（図２）

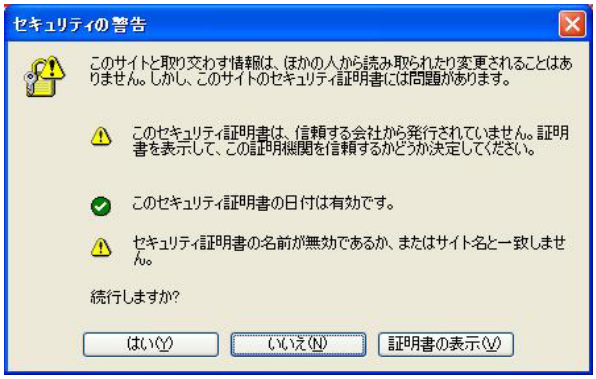



（図３）

図１から図３までは正規のサーバ証明書の例でしたが、以下では怪しさ満点の例をご紹介します。

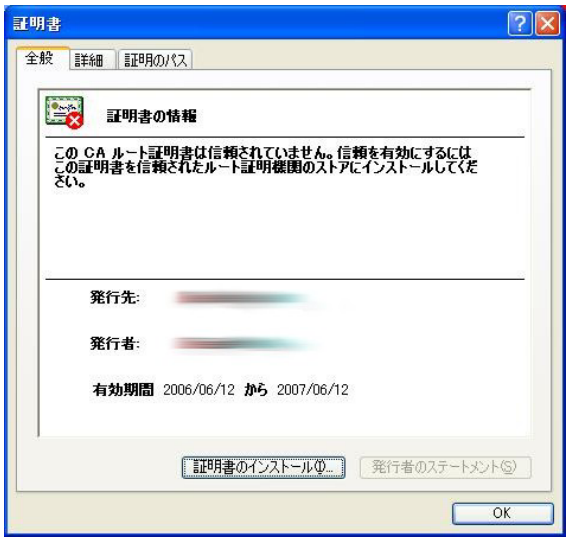
図４で怪しいURL（ホームページアドレス）を入力して実行すると、図５のような警告メッセージが表示されます。図５の警告は、１番上で「誰が（発行者）」が信頼できませんとの警告し、一番下で「誰を（発行先）」もおかしいと警告しています。（図５）


（図４）




（図５）

図５で「はい(Y)」をクリックしますとそのホームページが表示されますが、怪しいページなので、図２にある南京錠みたいなマークをダブルクリックしても、図６のように「このCAルート証明書は信頼されていません。…」と表示されます。（図６）




（図６）

## 4. ひるがえって大学では…

さて、一方大学ではどういう利用シーンがあるでしょうか？一例として挙げられるのは、各電算システムなどに、権限のある人だけが安全・確実にログイン（認証）できるような仕組みです。現在はログイン ID とパスワードを知っていれば誰でもシステムに入れることが出来ます。極端な話、私が総長や理事の ID とパスワードを知っていれば、総長や理事になりすますこともできます。しかし、PKI の技術を使い、本人しか持っていない鍵を使って各システムにログイン（認証）すれば、なりすましは絶対ありえません。そしてその鍵は厳重に保管しなければなりません。では、その鍵はどこに保管するのでしょうか？次にその一例がありました。

## 5. 「公的個人認証」の申請に行ってきました！！

疲れる話が続きましたので、ちょっと一休みです。

ある日、公的個人認証の申請をするため私が住んでいる市役所へ行ってきました。ここで、ほとんどの人が「公的個人認証？？？」と思われるでしょう。「公的個人認証」とは都道府県知事が大島大輔という私人（市民）に対して、電子的な身分証明書（以下、電子証明書）を作成してくれるものです。そしてその電子証明書は以下の住民基本台帳カード（以下、住基カード）の IC チップに格納されています。（図７）（図８）


（図７）

（図８）

図８は図７の拡大図です。この図８はリーダに接触するための電極ですが、この下に数ミリ角の IC チップがあり、そこに私の情報が格納されています。格納されている情報は、公的個人認証サービスポータルサイトによると、「氏名」、「住所」、「生年月日」、「性別」、「公開鍵」、「都道府県知事の電子署名」です。

申請当日の様子を書いてみます。なお、話をわかりやすくするため、市役所窓口の方と私のやり取りは、言葉の意味を少し変えてあります。

〇某月某日
私：「すみません、公的個人認証を申請したいのですが。」
役所：「はい、ではこの用紙に必要事項を記入してください。住基カードに載せる写真はどうしますか？こちらで撮影することもできますが。」
私：「はい、撮影もお願いします。」

公的個人認証の申請について補足しますと、まず私の情報を格納するための IC カードが必要です。それが住基カードです。一般の人はほとんど住基カードを持っていない（※注）ため（私もそうでしたが…）、まずは住基カードを発行してもらいます。そして発行後、電子証明書を格納してもらいます。格納と書くと大げさなような感じですが、役所の人が住基カードを専用のリーダ/ライタに挿して、あとはパソコンで簡単なデータを入力して、図８の電極の下にある IC チップに情報を書き込む（記録する）だけです。申請書に記入する内容は特に難しいものではなく、名前、性別、住所、生年月日、電話番号を記入して提出し、同時にデジカメで私の写真を撮影してもらいました。

※注　ほとんど住基カードを持っていない…
役所の人から聞いた話ですが、最近ではお年寄りが住基カードの申請をするそうです。なぜかというと、お年寄りは運転免許証などの写真入り身分証明書は持っていない場合が多いので、公的な身分証明書である住基カード（写真付き）の申請をするそうです。公的な身分証明書であるため、当然、運転免許証などと同じ効力があります。

さて、申請書を提出してから住基カードが作成されるまで、およそ 10 分くらいだったでしょうか。

役所：「住基カードを作成しました。続けて電子証明書を作成します。この住基カードに電子証明書を格納しますので、暗証番号を別室で入力してください。」
私：「暗証番号は何文字ですか？数字や記号は入力可能ですか？大文字小文字の区別はありますか？」
役所：「暗証番号は 4 文字以上 8 文字です。数字は可能ですが、記号は不可です。大文字小文字の区別はありません。」
暗証番号を入力するのはキーボードからではなく、アルファベットや数字のみがある画面にタッチするやり方でした。

以上で公的個人認証を取得することができました。時間は約 40 分でした。なお、手数料は自治体によって差があるかもしれませんが、私の住んでいる市は、住基カードが 500 円、電子証明書の作成が 500 円で合計 1000 円でした。

公的個人認証の主な用途として、インターネット上で税務申告をしたり住民票の写しを請求したりできます。

それでは、なぜオンライン（電子）申請で公的個人認証という電子的な身分証明書（電子証明書）が必要なのでしょうか？まず、現実世界においてみなさんが、役所に何かを申請しに行くときのことを思い出してください。運転免許証やパスポートなどの身分証明書と印鑑を持参しますよね？そして、窓口で役所の人があなたの身分証明書と（目の前にいる）顔をみて確かに本人だという確認をします。ところがデジタルの世界ではそのような確認方法はとれません。そこで、電子証明書を IC チップに格納し、その情報は役所のサーバに暗号化して送信され、申請を受けた役所側のサーバで確かに本人だという確認をするわけです。

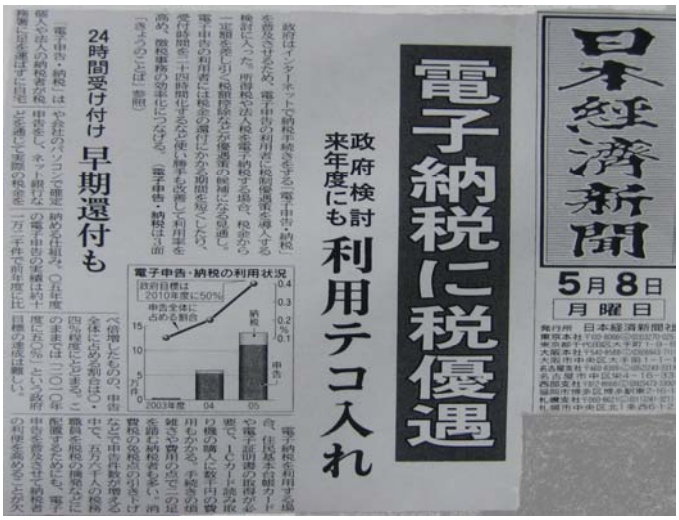
しかし、残念ながら公的個人認証は現在のところあまり普及していません。その理由として、

1)事前にある程度知識がないと申請しづらい
2)申請して公的個人認証を取得したのはよいが、利用するまでのハードルが高い
3)利用してもあまりご利益を感じられない

といった３点が主な理由であると私は考えています。

このうち「３」のご利益については、2006 年 5 月 8 日付け日本経済新聞（図９）によると、「電子申告の利用者に税制優遇策を導入する検討」に入り、「所得税や法人税を電子納税する場合、税金から一定額を差し引く税額控除などが優遇策の候補」らしいです。もうひとつのご利益としては、平成 19 年の確定申告より電子納税の受付時間を 24 時間にするそうです。各府省庁、自治体では、電子納税に限らず、オンライン（電子）申請をする利用者に対してのご利益を模索しているようです。

そして、我々PKI プロジェクトもみなさんのご利益になりそうな仕組みを色々試しています。


日本経済新聞
5月8日
月曜日
電子納税に税優遇
政府検討 来年度にも 利用テコ入れ
24時間受け付け 早期還付も
電子申告・納税の利用状況

（図９）©日本経済新聞　2006 年 5 月 8 日付け朝刊一面

## 6.PKI を運用するための情報基盤センターの体制

PKI はインフラ（蛇口を捻れば水が出て、スイッチを押すと電気が点くのと全く同じです）であり、決して表に出るような技術ではないと思います。表に出ないが故、皆さんが意識しなくても使えるような仕組みを作るのが情報基盤センターPKI プロジェクトの使命だと思います。

そして、ひとたび世の中に浸透すれば、なくてはならないものであり、きっとみなさんにご利益を感じていただけると確信しています。

これまでPKIの技術について説明してきましたが、そろそろ電子証明書の発行や運用体制について説明しなければなりません。それでは次回、情報基盤センターがどのような体制でPKIの運用をするかご説明します。

最後になりますが、総務部情報課の皆様にはPKIプロジェクトについて、ご理解、ご協力いただいていますことに感謝申し上げます。

参考：

東京大学情報基盤センターPKIプロジェクト：http://www.pki.itc.u-tokyo.ac.jp/
日本経済新聞：2006年5月8日付け朝刊一面
公的個人認証サービスポータルサイト：http://www.jpki.go.jp/
日本ベリサイン株式会社：https://www.verisign.co.jp/
ビートラステッド・ジャパン株式会社：https://www.betrusted.co.jp/
「PKI 公開鍵インフラストラクチャの概念、標準、展開」、カーライル・アダムズ、スティーブ・ロイド、ピアソン・エデュケーション、ISBN:4-89471-248-2, 2000

（大島大輔）