「技術だけでは信頼できないＰＫＩ(公開鍵インフラストラクチャ)」

２００２年5月

サートラスト株式会社　開発部
三崎友明

はじめに

普段の生活の中で高度な技術を利用しているのに非常に簡単に利用している道具も少なく無いと思います。
朝起きるとほぼ毎日のようにテレビをつけ今日の天気や世界中のニュースを手に入れる事ができますが、「何故、映像が映るのか？」「どうやって、地球の反対側の映像をリアルタイムで見る事ができるのだろうか？」そんな事を考えながら見る人もあまりいないでしょうし、利用者が気にする必要もあまり無いのでしょう。
放送局から自宅のテレビまでの間で第三者による情報改竄が行われる心配はまったく無いのでしょうか？
視聴者は放送局が提供する情報をどういう根拠で信頼しているのでしょうか？
放送局の社会的信頼、法律で守られている、アナウンサーの顔が見える、有名な解説者が言っている、ニュース番組である、他の放送局も同じ情報を提供している、など技術的なこと以外にも視聴者が情報を信頼するために必要なものがあるのだと思います。
同様にＰＫＩ利用者が詳細な技術的仕組みを知らなくても簡単な操作で、かつ安全に利用できるようになるためには、ＰＫＩの技術的信頼の現状や限界を知り、便利性と引き換えになるリスクを極力減らすために利用者が必要とする最低限の知識を考えていくことを目的としています。

１．鍵

ＰＫＩの中でも電子署名が注目を浴びていますが、電子署名を知るにはまずは暗号を知らなければなりません。
電子署名とは［公開鍵暗号］をうまく利用した方法だからです。
まずは、暗号にとって重要な「鍵」について考えていきたいと思います。

１－１．共通鍵暗号

ＰＫＩの本を見ると共通鍵や公開鍵、秘密鍵といろいろ「鍵」が出てきます。
では実際に「鍵」の例を見てみよう。

「81DC9BDB52D04DC2」

何だ、英数字だけじゃ無いかと思われるかもしれませんが、いわゆるパスワードと同じように単なる文字列が入ったファイルなどがほとんどです。
パスワードと言うと操作する人が忘れないような言葉や数字を利用する場合が多いですが、コンピューターの場合、利用者が誤って消去するか故障でもない限り忘れる事がありません。
パスワードやランダムに発生させた文字列を「鍵」と言っているだけです。

よく鍵長○○○ビットと言う言葉を聞くと思いますが、この鍵の文字数を表しているもので上記例では１６文字ありますから１文字には８ビット必要なので「8 x 16 = 128 ビット」と言うことになります。
なんだ１０２４ビットより少ないから駄目じゃないか！思われる方もあるかもしれませんが、そうではありません。
「鍵」を使って利用する暗号プログラムにもいろんな種類があり、利用する「鍵」の長さが違ったり、いくつか異なる長さの「鍵」が使えたりします。
また暗号プログラムによっては１２８ビットでも十分な暗号強度があるが、逆に５１２ビットあってもまだ不十分と言われるものもあります。
これは、それぞれの暗号プログラムの特徴や用途によって違ってくるもので、どれが最も良い暗号プログラムと言うものではありません。

では、実際に「鍵」を利用してみましょう。

「元の情報」"本日は晴天なり"
↓
「暗号プログラム」← 「鍵」"81DC9BDB52D04DC2"
↓
「暗号情報」
"mgemC9VotUQNU7SpOzLhi7tq+S5sij96ToVZCoMSwErr9ZEm+uod6u5eEp78OQ7j"
"ZgbO6x+li5nOOllMGRix+c5CcqJunufgRY9tNQyYOq8Pj9lr5jnq8+q2eanhnS4P"
"5skT129BOfInCJ5Fzl9qVtLihXbsTpf6U7nSbz1Tlf8="

「元の情報」を「暗号プログラム」と「鍵」を使い「暗号情報」に変換しました。
では、「鍵」を使って「暗号情報」から「元の情報」に戻してみましょう。

"mgemC9VotUQNU7SpOzLhi7tq+S5sij96ToVZCoMSwErr9ZEm+uod6u5eEp78OQ7j"
"ZgbO6x+li5nOOllMGRix+c5CcqJunufgRY9tNQyYOq8Pj9lr5jnq8+q2eanhnS4P"
"5skT129BOfInCJ5Fzl9qVtLihXbsTpf6U7nSbz1Tlf8="
「暗号情報」
↓
「暗号プログラム」← 「鍵」"81DC9BDB52D04DC2"
↓
「元の情報」"本日は晴天なり"

今回の例のように、「暗号する場合」と暗号した情報を元に戻す「復号する場合」で、同じ「鍵」を利用する方法を「共通鍵暗号」と言います。
２者間で暗号通信を行う場合には、２者とも同じ「鍵」を持っている必要があります。
また、ＡとＢ以外の「鍵」を持たない第三者が「暗号文」を入手できたとしても「文章」に変換する事は困難であり、同じ「鍵」を持つＡとＢの間では「盗聴」される心配が低いことがわかります。

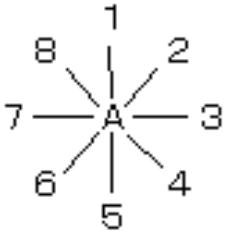
A　　B
「文章」――――――――――＞「暗号文」――――――――――＞「文章」
「鍵」　　「鍵」

１－２．鍵の重要性

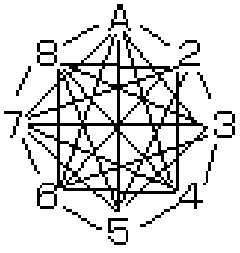
１－１でお互いに同じ「鍵」を使い暗号文で安全に通信を行うお話をしました。
しかし、ＡとＢの間で「文章」を「暗号文」にして「盗聴」の心配無く安心して伝えるにはまず、共通の「鍵」をあらかじめＡ、Ｂの両者が持っている必要があります。
たとえば「鍵」をＦＡＸや手紙、手渡しなどで確実に相手に伝えなければなりません。
電子メールで「鍵」を送るなどはもってのほかです！
もし電子メールが盗聴され他人に「鍵」が伝わってしまっては、せっかく「暗号文」を使っていても簡単に解読されてしまいます。
ＡとＢの両者は「暗号」を使い安全に通信を行っているつもりでしょう、本人たちは絶対に第三者には伝わらないと安心しきったまま、通常の通信では行わないような情報までも・・・

あと、Ａが「暗号」で通信を行う相手がＢだけであれば良いですが、他にも複数の人と「暗号」通信を行うとなると、それぞれの相手に共通の「鍵」が必要となり膨大な数の「鍵」を管理しなければならなくなります。

Ａが８人からもらう暗号文の解読には８個の「鍵」が必要となる。



８人がそれぞれ暗号文の通信を行う場合は膨大な「鍵」の数が必要となる。



１－３．公開鍵暗号

「鍵」を「公開」する？大事なものを何故？
と思っていただければまず１－２は理解していただいたのだろうと思います。
では「公開鍵暗号」の「鍵」を実際に見てみましょう。

鍵１

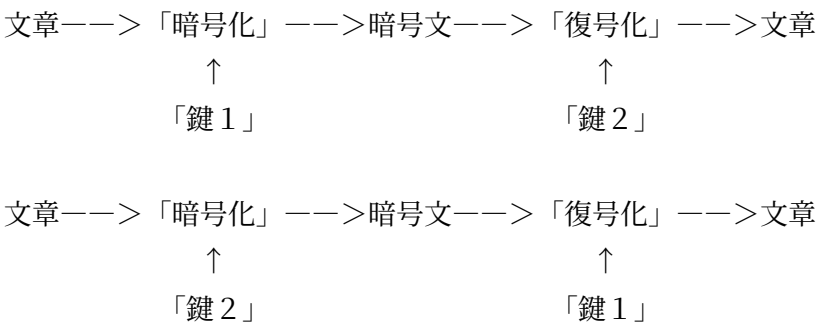
AAF7238F7A8CD93ABD39904094ECA443BA6D3298275917546F49A0868175BCF76919
B592ECC29F700DEF18B701F6DD5E2134EBA3209923664EB8821E59435A63

鍵２

7414CDAE53D56281818D9E265B77B9A8CAE1EDE2658516541C23EFBCA4161F30F9A8
EAEE3AB1E934AE8DD734FEEE93970F91AA86EEC9592E592E304E5AA83D81

えらく長い「鍵」で、なぜか２つも鍵があります。
長い「鍵」であることは「公開鍵暗号」の特徴のように見えますがそうではありません。
「公開鍵暗号」のもっとも一般的なものが「ＲＳＡ暗号」であり、「共通鍵暗号」の代表的なもの「ＤＥＳ暗号」に比べれば「鍵」を長くしなければ強度が保てないと思われているからです。
もしかすると今後発明される「ＲＳＡ暗号」に代わる新しい「公開鍵暗号」の仕組みは、非常に短い「鍵」でも今より強度の高い暗号となるかもしれません。

あともうひとつ「鍵」が２つあるという事が「公開鍵暗号」で最大の特徴です。
この２つの「鍵」は、どちらかの「鍵」で暗号化したものは、もう片方の「鍵」でなれれば元に戻すことができません。
たとえば「鍵１」で暗号化してしまった文章は暗号化に使った「鍵１」では元に戻りません。
「鍵２」を使うと元の文章に戻すことができます。
逆に「鍵２」で暗号化を行った文章は「鍵２」では戻りません、「鍵１」を使うと元の文章に戻すことができます。



「鍵１」と「鍵２」の２つの「鍵」の特徴を理解していただけましたでしょうか？
では、鍵の片方どちらか「鍵２」を一般公開してしまいましょう！！
「え？」と思わず、もう一度、考えてみてください。
「鍵２」を誰もが見ることのできるインターネット上に公開しました。
知らない人でも自分の「鍵２」を持っているかもしれませんが、「鍵２」だけで出来る事は「暗号化」するだけです。
しかも「鍵２」で暗号化されたものは、公開されている「鍵２」では解読できません。
つまり「私宛の暗号化通信には「鍵２」を使って暗号文にして送ってください。」となり送ってもらった「暗号文」は公開していないほうの「鍵１」でしか元にもどせません。
だから「鍵２」は公開するが「鍵１」は誰にも公開してはいけません！！

この「鍵」の扱い方から公開する「鍵２」を「公開鍵(**Public Key**)」と呼び、公開しないほうの「鍵１」を「秘密鍵(**Secret Key, Private Key**)」と呼んでいます。
また「鍵」が２つあるので、２つの鍵セットを「ペア鍵」とも呼ぶようです。

１－２では「共通鍵暗号」の２つの問題点であるところを「公開鍵暗号」で考えてみましょう。

１．相手にいかに安全に「鍵」を渡すか？
「公開鍵」は他人に知られても問題が無いのでホームページや電子メールで送って他人に知られたとしても問題は無い。

２．相手が複数になると膨大な「鍵」の数になってしまう。
自分の「公開鍵」を他の人に渡し、自分宛にはその「公開鍵」で暗号化をしてもらう。
暗号文を相手に送るときは、その相手の「公開鍵」をもらう必要がある。
・自分の鍵は「公開鍵」と「秘密鍵」の２つがある。
・相手の鍵は「公開鍵」を相手の数だけ持つ事になり、送る相手の「公開鍵」で暗号化する。

１－４．電子署名

１－３で「公開鍵暗号」について説明しましたが、もう一度「公開鍵」と「秘密鍵」の特徴を思い出してください。
　「公開鍵」で暗号化したものは「秘密鍵」でしか復号化できません。
もうひとつの特徴
　「秘密鍵」で暗号化したものは「公開鍵」でしか複号化できません。

ここに「公開鍵」で複号化できる「暗号文」があったとすると誰がこの暗号文を作ったのでしょうか？
「秘密鍵」は自分しか持っていません。
つまり「暗号文」を「公開鍵」でもとに戻せたという事実が「秘密鍵」の持ち主が行った行為である証拠となるのです。

簡単に整理しましょう。
１．「公開鍵」で暗号化した「暗号文」は「秘密鍵」の持ち主しか元にもどせない。
　　→ 公開鍵暗号
２．「暗号文」を「公開鍵」で元に戻せた場合、「秘密鍵」の持ち主が出した情報である。
　　→ 電子署名

１－５．誰の公開鍵？

「公開鍵暗号」を使うことによりネットワーク上でもかなり安心して暗号化や署名が使えそうな感じになりました。
ところが、もう１つ問題があります。
「公開鍵」をもらうときに、この「鍵」は誰の「公開鍵」であるか？という問題です。
たとえば、Ａの「公開鍵」だと思って「暗号文」を作成したが、実はＡのふりをした偽者Ａの「公開鍵」かもしれないのです。
Ａしか読めないはずの「暗号文」も偽者の「公開鍵」をもらってしまったために偽者Ａに読まれてしまうのです。
では、どうやって正しいＡの「公開鍵」を手にいれるか・・・・・
１．Ａと直接会って「公開鍵」をもらう
２．直接会ったＢの「公開鍵」があるので、Ｂの署名付でＡの「公開鍵」を送ってもらう。
２の考え方はＰＧＰという暗号、署名ツールで採用されている方法です。
ところで、Ｂは、どうやってＡの「公開鍵」を手にいれたのだろうか？

もしかすると、ＢからもらったＡの「公開鍵」が偽者Ａの「公開鍵」だったらＢに責任を取ってもらうのか？

誰の「公開鍵」であるかをチェックしてくれるだろうと言うところが「認証機関」または「ＣＡ」、「認証局」と呼ばれているところです。
「認証機関」は申請された「公開鍵」が申請者自身であるかの認証を行い本人であれば「証明書」と「公開鍵」に対し「認証機関」の「秘密鍵」で電子署名を行います。

Ａ	認証機関
「公開鍵」 ―――――――＞	本当にあなたはＡさんですか？ 登記簿謄本を見せてください。 住民票など身分証明書を見せてください。

「認証機関」はあらゆる手段により「公開鍵」がＡであるかを確認している。
その確認方法や手段などは「認証機関」により異なる。

Ａ	認証機関
「証明書」＜―――――――	どうやらあなたはＡさんのようですね？ あなたの「公開鍵」を「認証機関」の「秘密鍵」で署名しましょう。

「証明書」には何が入っているのでしょうか？
これも「認証機関」により違うでしょう。
一般的な証明書であればこのような情報が入っているようです。

・証明書を発行した認証機関名や認証サービス名
・申請者の名前などの情報
・証明書の有効期間
・証明書の用途
・申請者の「公開鍵」

1998 年 9 月 4 日（現地日付）アイルランド ダブリンで、クリントン米大統領とアイルランドのバーティ・アハーン首相が両国間で合意した電子商取引に関する共同声明に電子署名を使ったようです。
電子署名を使うのであれば両者が同じ場所に集まらなくても良いと思いますが、いろんなパフォーマンス的な事もあったのでしょうね、それは良いとして米大統領、アイルランド首相の双方が「ペア鍵(秘密鍵,公開鍵)と証明書」が入ったＩＣカードを使い電子文書に対し電子署名を行ったあと記念にＩＣカードを交換したようですね。
その後、アイルランド首相が米大統領に成りすまして電子商取引を行ったかどうかは、さだかではありません(笑)

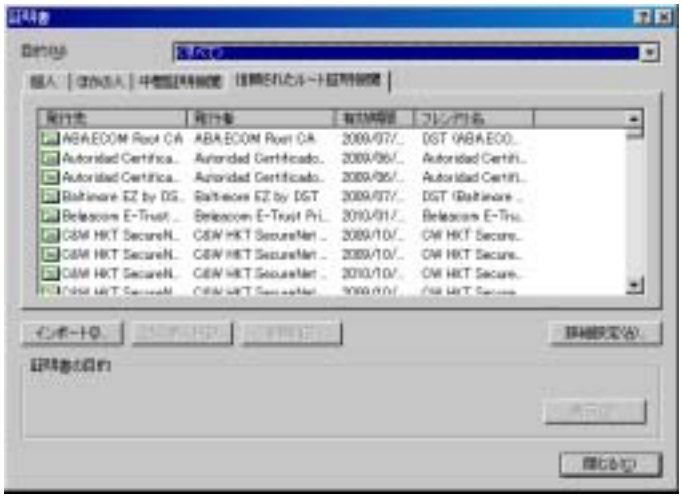
最後に念を押しますが「公開鍵」が誰のものであるかを「認証機関」が保障しているもので言わば「公開鍵の身分証明書」のようなものが「証明書」です。
「証明書」や「公開鍵」は見ず知らずの人に渡してもかまいませんが、「秘密鍵」は絶対他人に渡してはいけません。
実印が今どこにしまってあるか覚えておくように、常に自分の「秘密鍵」がどこに保存されているのか注意しましょう。
今後、日本が諸外国と電子署名を使って調印するときは是非とも注意して欲しいですね。

１－６．認証機関の証明書

もう一度、証明書の発行から、署名の検証まで鍵の動きを順に確認して見ましょう。
証明書の発行
１．利用者Ａはペア鍵(秘密鍵と公開鍵)を作成し、認証機関に対し「公開鍵」を提出
２．認証機関は提出された「公開鍵」とＡ本人であるか確認を行う。
３．認証機関の「秘密鍵」でＡの「公開鍵」に署名を行い「証明書」を作成する。
４．認証機関は署名した「証明書」をＡに渡す。

電子署名
１．Ａは「秘密鍵」で文章に署名を行い、署名と証明書をＢに渡す。
２．Ｂは証明書が信頼する認証機関か確認するために「認証機関の公開鍵」で証明書の署名を検証する。
３．証明書内に入っているＡの公開鍵でＡの署名を検証する。

だれの公開鍵であるかを認証機関が証明してくれるとありますが、では認証局の公開鍵はだれが保証するのでしょうか？
実際には認証機関は自分の公開鍵を自分の秘密鍵で署名した証明書を発行しています。
この証明書は自分で自分を署名しているので自己署名と呼びますが、他の誰も保証しない自分で自分を保証している証明書なのです。
結局は認証機関が発行する自己書名の証明書をまず安全に手に入れなければなりません。
しかし、普段つかっているブラウザなどには、既にこの認証機関の自己署名証明書がインストールされている為にわざわざ手に入れる事が無いのです。



Microsoft Internet Explorer に最初からインストールされている認証機関の証明書です。
とりあえずは、信頼のおける認証機関の証明書さえ手元にあれば、その認証機関が発行する証明書を持っている人の署名は、ある程度の信頼を技術的に保証できることになります。

２．信頼の限界

公開鍵暗号の暗号文や電子署名を受け取ったときの検証方法を大まかに理解してもらったとして技術的に信頼できたとしても、それを信用するにはリスクが伴います。
利用者が次のリスクを理解した上で信用するか信用しないかを判断しなければなりません。
しかし、現状のアプリケーションでは技術的に信頼されると無条件に信頼されてしまい利用者にはリスクのある事をまったく知らせていないようにも思います。

２－１．秘密鍵の盗難、紛失など

最初に、認証機関が秘密鍵と公開鍵を作成し利用者に証明書と一緒に配布していてはどうでしょうか？
「秘密鍵を紛失しても認証機関やその他の機関がバックアップしていますので安心です」と平気で説明しているところには驚いてしまいます。
これは、利用者がまだＰＫＩに慣れておらず、秘密鍵の紛失やパソコンの設定が不慣れであるために、これを提案しているベンダーさんや認証機関の気持ちは十分にわかるのですが最もやっては行けない事だと思います。
利用者の為と言いながらも実際にはサポートが大変だからじゃ無いでしょうか？
もちろん、バックアップの重要性は判りますが、それでも秘密鍵は本人にしか利用できないバックアップを考えるべきだと思います。
あと、現状では秘密鍵をパソコンの中に保存するケースが最も多いと思いますが、パソコン自体の盗難や３章で説明しますが秘密鍵の利用にパスワードが設定されていない場合などは非常に危険です。
証明書を取得する際やバックアップしてある証明書をインストールする際には、秘密鍵の利用にパスワードを必要とする設定やインポートした秘密鍵をバックアップ不可能にする設定など自分の秘密鍵は自分で守りましょう。

この秘密鍵が紛失や盗難にあった場合はクレジットカードの紛失と同様です。
他人に悪用されないように速やかに認証機関に紛失の届けを提出しましょう。
とは言っても今の時点では悪用される先も無いでしょうが必要ある知識と思います。
「秘密鍵」を紛失や利用しなくなった場合は、「秘密鍵」とペアになっている「公開鍵」も利用できなくなったので、「公開鍵の身分証明書」である「証明書」の失効（無効）を認証機関に申請します。
認証機関によっては破棄理由を聞かれる場合がありますが、これはかなり重要です。
たとえば、利用しなくなった「秘密鍵」であれば単なる失効ですが「紛失」となれば、過去にその証明書が保障する「公開鍵」と「秘密鍵」を利用した署名などは全て信頼できない可能性が発生します。

「秘密鍵」を手に入れてしまえばパソコンの日付を過去に戻し、過去の署名を作成できてしまうからです。
最近では時刻認証サービスなど署名した日時を第三者が保証してくれる公証役場のようなサービスもあるようです。

また、認証機関は失効申請された証明書のシリアル番号のファイルを署名し公開していますが更新までは認証機関により違いがあり、失効申請したとしても直ちに失効リストには反映しません。
失効リストには次回更新日時と言うものが入っておりこの日時までは更新をしなく、失効リストを公開しているサーバーの負担を低くしているのでしょう。
OCSP と言うリアルタイム性を重視した方法でも実際には、破棄リストを参照し回答しているだけで、破棄リストが更新されるまでは古い情報の可能性があります。
認証機関によってはこの失効のリアルタイム性を「売り」にして差別化をはかるものも出てきて良いと思いますね。

他にもうひとつ、重要な秘密鍵があります。
認証機関の秘密鍵で、認証機関内では最重要扱いにはなっていると思いますが、扱うのは人間です。
作業者への手順、監査やミスへの危機管理などが重要ですし、認証機関の秘密鍵が盗難にあった場合に過去の証明書も発行される可能性があるためです。
認証機関も自社のみで証明書を発行せず、認証機関同士で互いに時刻署名などを行い、せめて過去に発行した証明書だけでも信頼性を失わない方法などを考えるべきかもしれません。

あと認証機関の証明書は誰でも手に入れる事が可能です。
有名な認証機関ほどほとんどのブラウザに予めインストールされています。
この認証機関の証明書から公開鍵をとりだし、この公開鍵から秘密鍵を見つけ出すことは不可能なのでしょうか？
現状では公開鍵暗号にはＲＳＡ暗号が利用されており、鍵の長さは１０２４ビットから２０４８ビットになってきています。
確率から考えれば天文学的確率でなければ鍵は発見できなく、そんな事を心配するようでは外も心配で歩けないようなものだとは思いますが、コンピューターの性能向上も著しくＲＳＡ暗号を解く画期的なアルゴリズムが発見される可能性もあります。
認証機関の証明書は１０年ぐらいの有効期間があるものがほとんどです。
この数字は長いようにも思いますがどうなのでしょうか？

２－２．認証機関の認証ミスによる本人以外への証明書発行

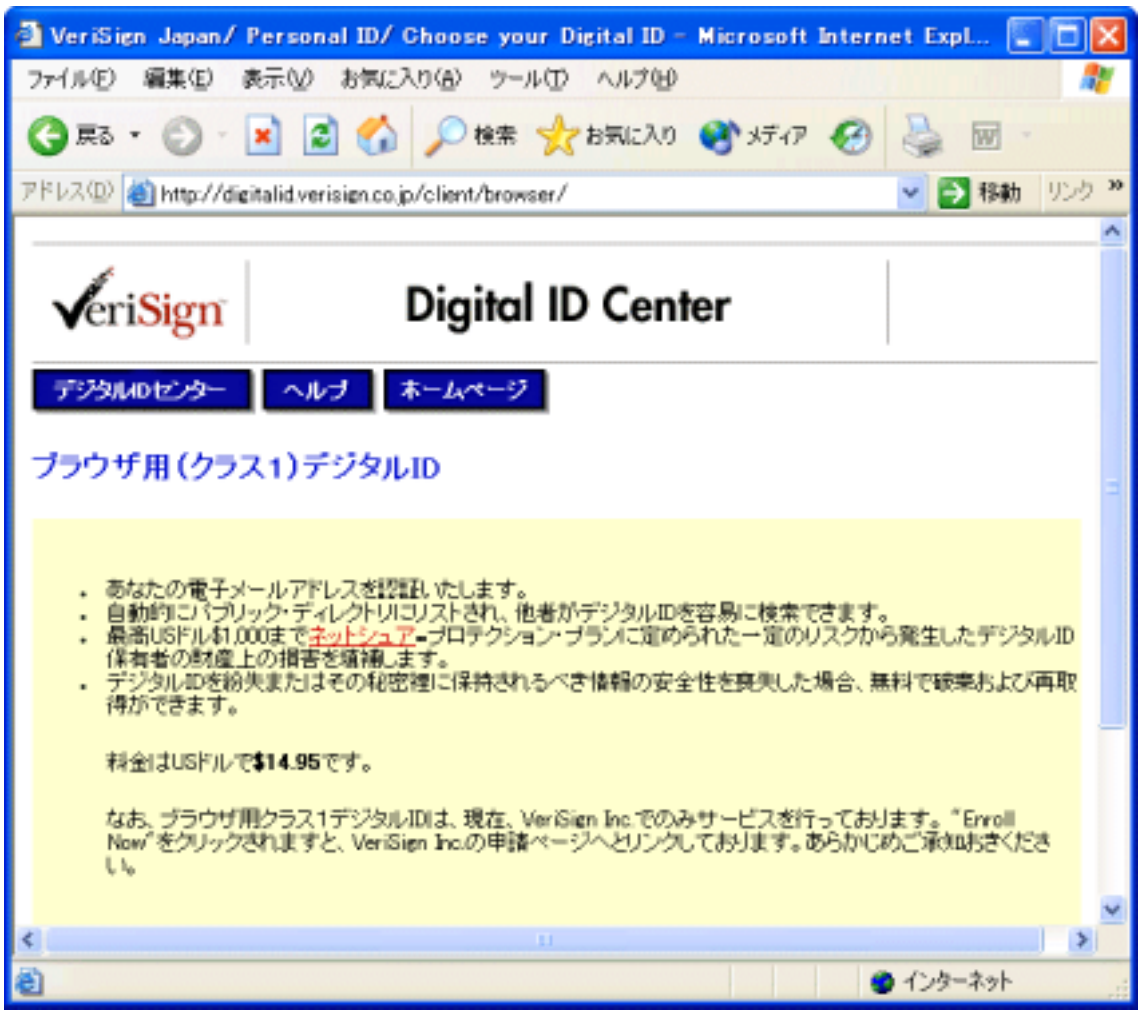
この事件は既に発生していますね。
米ベリサイン社がマイクロソフト社以外にマイクロソフト社の証明書を発行してしまいました。
技術的な検証だけでは偽者の証明書を信頼してしまいますね。
マイクロソフト社は米ベリサインの認証機関証明書を無効にする設定を公開していましたが認証機関にとっては致命的な対応と言えるでしょうね。
認証機関の提出者の認証方法に問題が無かったのか、認証方法自体が正しく守られているのか、またヒューマンエラーがあった場合にその検出は可能なのかが問われる事になると思います。

もちろん、認証機関が正しく認証したとしても偽者である可能性は否定できませんね。

A 認証機関では電話と郵便物により本人の存在確認を行っています。
B 認証機関では本人確認のために戸籍謄本と印鑑証明が必要です。
C 認証機関では実際に窓口まで来てもらって身分証明書を提示してもらわなければ
　発行手続きを進める事ができません。

あなたは、どの認証機関を信用しますか？
電子署名法で問題が無ければとりあえず何処でもかまわない？
ブラウザに入っている認証機関の証明書にはほとんど認証を行っていないものまでも含まれています。
PKI のソフトウエアーが「署名が正しいです」と表示されたので相手をまったく疑わず信頼しても良いですか？

認証機関によってはトラブルをある程度、金銭的に保障してくれるものがあります。



２－3. 認証機関の証明書

自分が持っている認証機関の証明書が違うものである可能性があります。
ブラウザをインストールすれば最初から入っているものがありますが、そのまま信頼するとブラウザソフトメーカーに信頼する認証機関の選定を委任していることになりますね。
IE では信頼されるが Netscape では信頼できないと表示されるなどブラウザのメーカーによっても信頼する認証機関が違ってくる可能性があります。
あと、ウイルス等によりあとから認証機関の証明書を入れ替えられる危険はないのでしょうか？
ブラウザソフトメーカーは何を根拠に予めインストールしてある認証機関を決めているのでしょうか？
技術的要件とあとお金？

もうひとつ、ブラウザに予め入っていない認証機関の証明書の場合はあとからインストールするしかありません。
あとからインストールすると言う事は、間違いなくその認証機関の証明書であるかを確認する事が重要です。
安易に「はい」を押してはいませんか？

３．おまけ

３－１．ＰＫＩを導入するとパスワードはなくなる？

結論から言えば無くならないでしょう。
しかし、いままでのＩＤとパスワードとは仕組みが大きく異なります。

たとえば、ＩＤとパスワード方式で認証を行いサーバーに接続した場合は、ＩＤとパスワードの有効性を確認しているのはサーバーです。
ＩＤとパスワードは通信回線を伝わりサーバーに送られていますし、サーバー側はもともと、その人のＩＤとパスワードを持っています。
利用者がＩＤとパスワードの管理をしっかりしていたとしても、サーバー側のＩＤとパスワードの管理がずさんであればまったく意味がありません。

利用者　　サーバー
ＩＤ、パスワード ――――――――――――＞ ＩＤ、パスワード　＝　ＩＤ、パスワード
利用者が提出したＩＤとパスワードが
サーバーが持っているＩＤ、パスワード
と一致するかを検証する。

そういえば最近、派遣社員が企業内で個人情報を盗みだし顧客の情報から不正にＩＤとパスワードを見つけ出す事件がありましたね。
パスワードはどうしても利用者が覚えやすいものになりやすく、ＩＤさえわかってしまえばサーバー側にＩＤと予想したパスワードで試してみることができてしまいます。

ＰＫＩで主に利用されるパスワードはちょっと違います。
いままでに「秘密鍵」の重要性を理解していただいていると思いますが、この秘密鍵はファイルなど電子的情報としてパソコンの中に入っています。
これでは、他人が勝手にパソコンを利用した、パソコンが盗難にあった、等の場合に非常に危険です。
そこで「秘密鍵」を「共通鍵暗号」＋「パスワード」で暗号化して保存しておく方法があります。
「共通鍵暗号」ですから元に戻すには暗号化した時と同じ「鍵」が必要です。
「パスワード」で暗号化すれば、同じ「パスワード」で元に戻せるわけですね。
具体的なやり方についてはまたの機会に。

この方法により普段「秘密鍵」は暗号化されているため、そのままでは利用できません。
利用するときだけパスワードを入力し「暗号化された秘密鍵」を元にもどして利用するのです。
つまり、このときのパスワードは自分のパソコンの中だけでしか利用されていないのです。
同様にＩＣカードも中にある「秘密鍵」を利用する時はパスワードを求めるものがありますが、ＩＣカードの場合は「暗号化された秘密鍵」をコピーするだけでも大変なのでさらに安全と言えるかもしれませんね。
ＩＣカードによっては、このパスワードを何度か間違えると中に入っている「秘密鍵」を自動的に消してしまう機能があるそうです。
しかし、ＩＣカードが壊れてしまった、などの場合に備えてバックアップを作りにくいと言う事もあるので薦めるにはちょっと悩むところです。

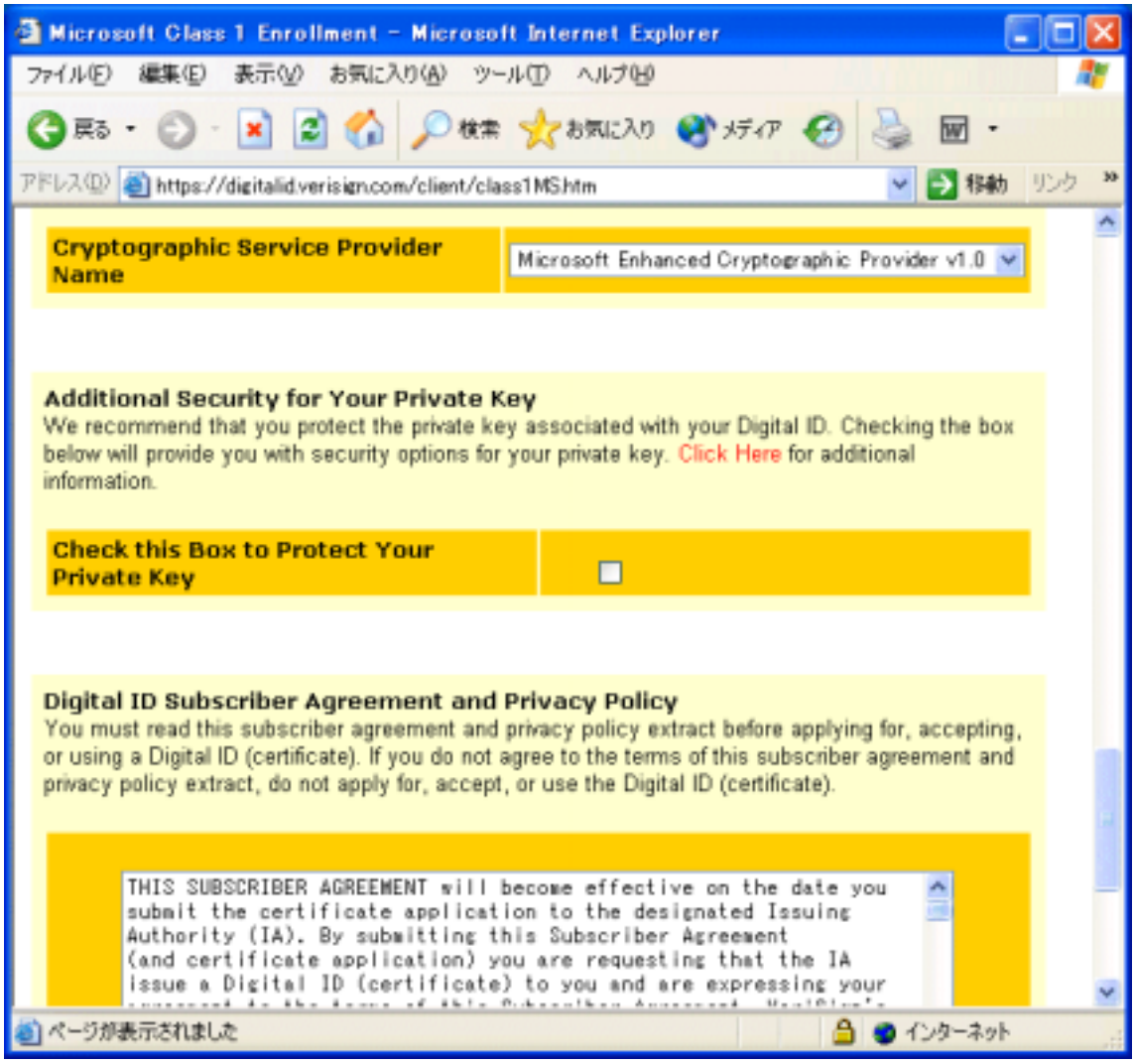
利用者　　サーバー
「証明書」　――――――――――――――＞ 信頼できる認証機関が発行した証明書？
＜―――――-――――― ランダムな文字を作成し電子署名を要求
「暗号化された秘密鍵」を
パスワードで元にもどす。
「秘密鍵」で署名　――――――――――＞ 電子署名が「証明書」内にある公開鍵で
複号できるか？
ＯＫの場合に利用者の接続を許可する。

サーバー側にはパスワードが保存されていません。
また「秘密鍵」で署名された情報がサーバーに届いているので利用者が接続したことの有力証拠となるでしょう。
ＩＤ、パスワード方式とは違い、もしパスワードが他人に知られたとしてもパソコン本体やＩＣカードが無ければ「暗号化された秘密鍵」を手に入れることができませんのでサーバーにそのパスワードを送ったとしてもまったくの無意味です。
逆にパソコンやＩＣカードが盗難にあったとしても「秘密鍵」を使われてしまうには「パスワード」が必要です。
もちろん、安易なパスワードにしておくのは良くありませんが、せめて盗難にあった事に気がつき「秘密鍵」を失効させる時間を稼ぐことができるかもしれません。

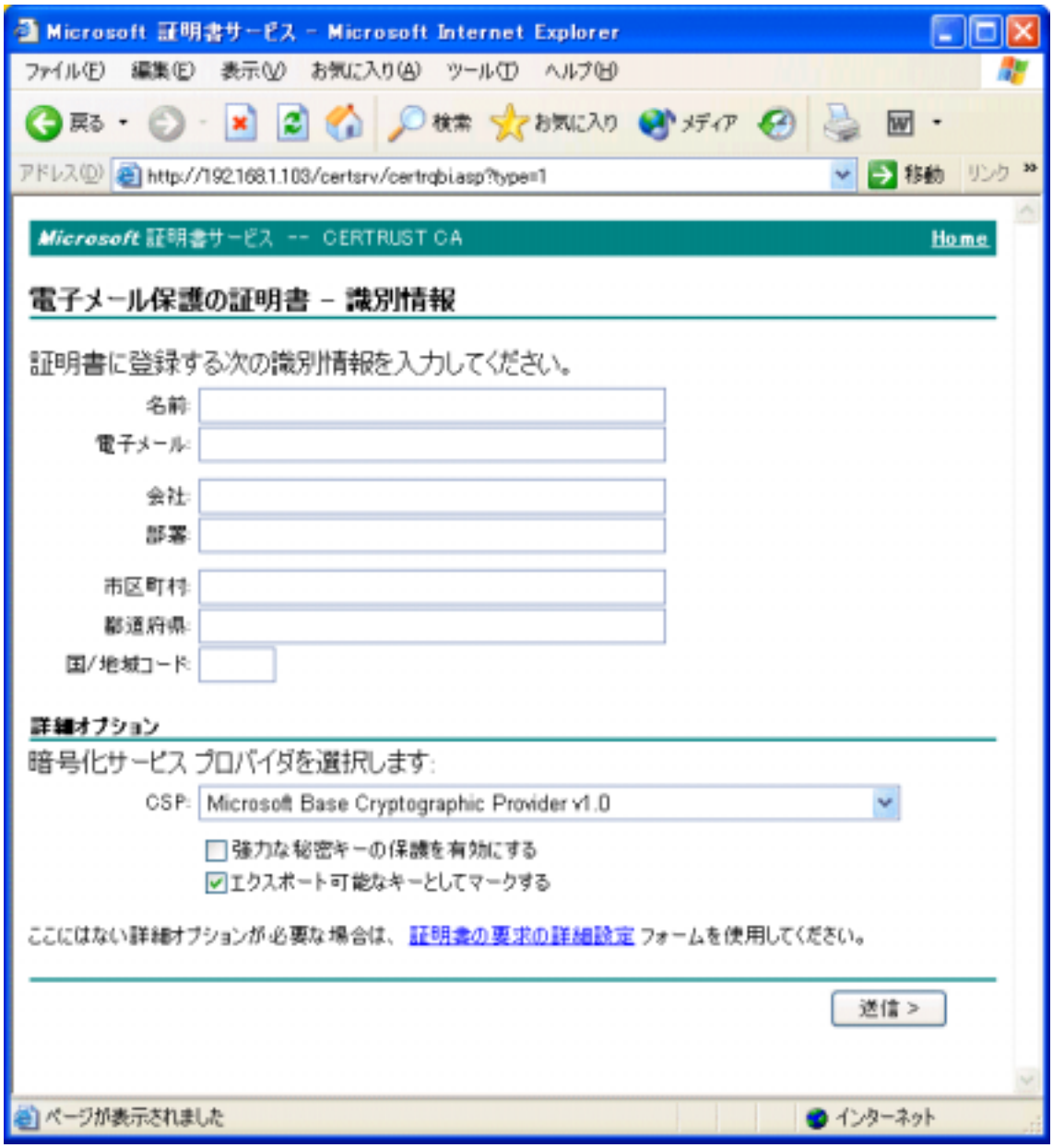
３－２．秘密鍵の管理

米ベリサイン社 Class1（ベリサインでは認証レベルで信頼の度合いをクラス別に表している）デジタル ID 取得画面です。
（デジタル ID はベリサイン社の登録商標です）

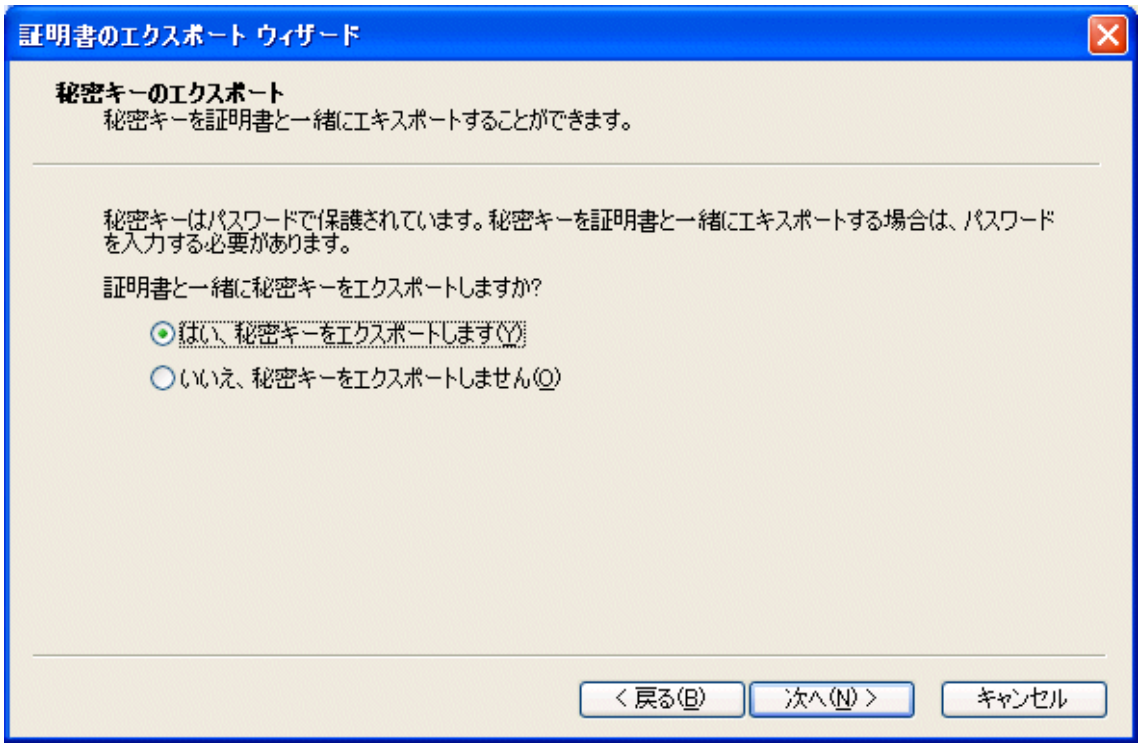
「Check this Box to Protect Your Private Key」をクリックすると、この証明書申請時と同時に作成される「秘密鍵」をパスワードで暗号化しハードディスクに保存します。
電子署名など「秘密鍵」を使うときはパスワードを入力しなければ利用できません。



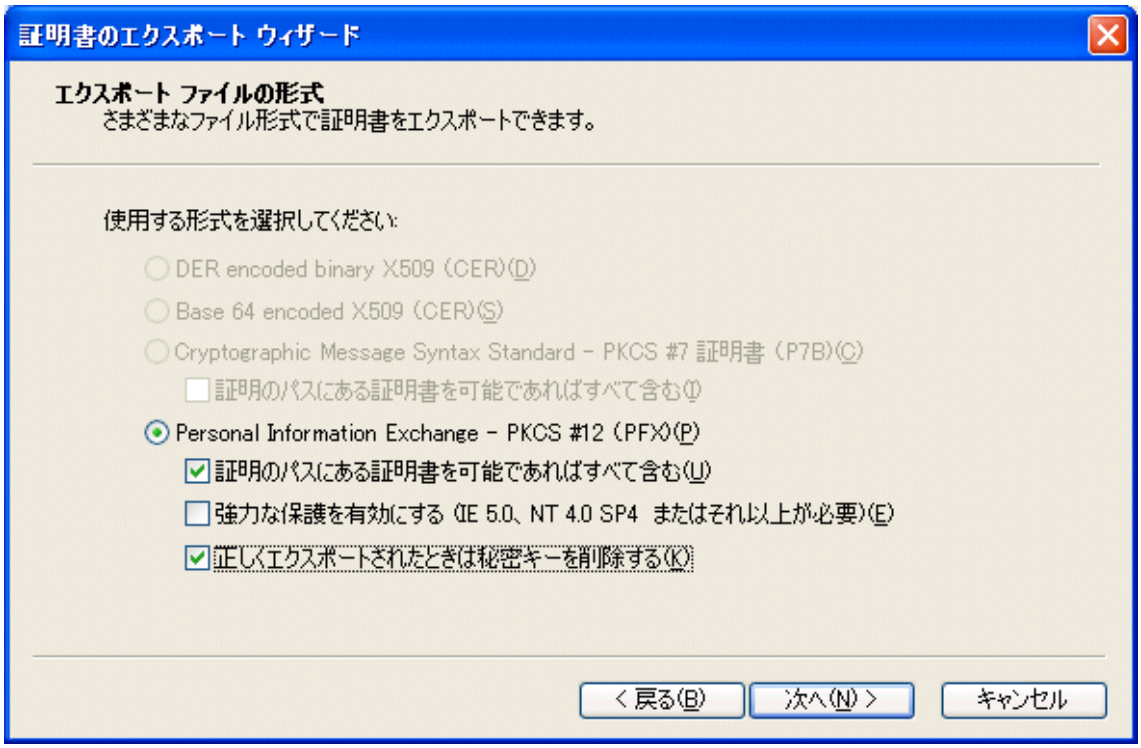
Microsoft Windows2000 Server に付属している証明書発行サービスプログラムです。
無償なので是非利用して PKI を実感してみましょう。
証明書を取得する際に「強力な秘密キーの保護を有効にする」をチェックすると、この証明書申請と同時に作成される「秘密鍵」をパスワードで暗号化してハードディスクに保存します。
「エクスポート可能なキーとしてマークする」はチェックすると「秘密鍵」のバックアップが出来なくなってしまいます。
ある意味､安全ではありますが､ハードディスクの故障や OS の再インストールを行うと｢秘密鍵」も消えてなくなってしまいますね。



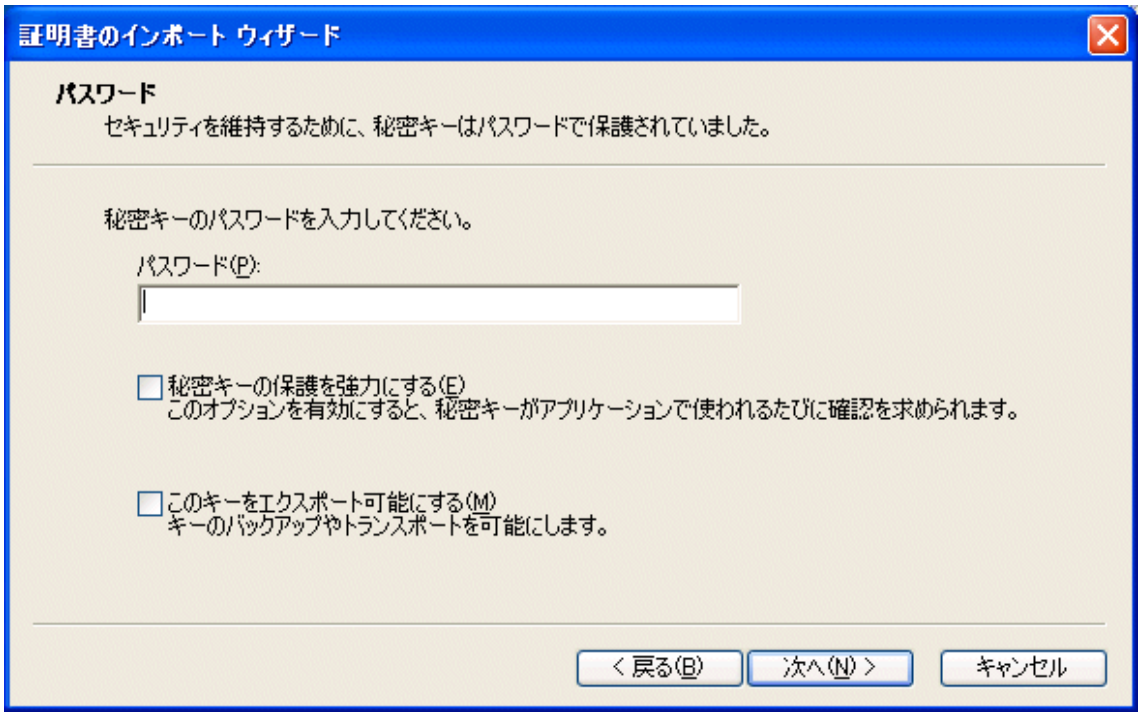
秘密鍵のお勧めのバックアップ方法ですが、まずブラウザで取得した場合、実際にはブラウザで申請すると同時に「秘密鍵」と「公開鍵」を作成し、認証機関に「公開鍵」を提出しています。
IE の場合であれば、タスクバーのメニューから「ツール」「インターネットオプション」「コンテンツ」「証明書」を選び、「個人」の証明書の中でバックアップしたい証明書を選択します。
IE の場合、この「個人」に入っている証明書は、実際には「秘密鍵」+「公開鍵」も証明書と一緒になっています。
「エクスポート」を選択し「証明書のエクスポートウイザード」を開始します。
「秘密キーのエクスポート」では「秘密キーをエクスポート」を選択します。



「証明書のパスにある証明書うぃ可能であればすべて含む」と
「正しくエクスポートされたときは秘密キーを削除する」をチェックしファイル名を指定して、「秘密鍵」「公開鍵」「証明書」「認証機関の証明書」をバックアップします。
このバックアップしたファイルはフロッピーなどにコピーして大切に保存しましょう。



こん度はバックアップした「秘密鍵」を再度インストールします。
今度は「インポート」を選んで先ほどバックアップしたファイルを指定してください。



「秘密キーの保護を強力にする」をチェックして「このキーのエクスポート可能にする」はチェックを外してインストールすると「秘密鍵」利用するにはパスワードが必要で、しかもこの「秘密鍵」はバックアップが不可能になっています。

４．最後に

PKI 自身まだまだ実用されているとは言いがたいものがありますね。
何が普及を拒んでいるのでしょうか？
セキュリティ的なものは確かにまだまだかもしれませんが１００％確実なセキュリティは存在しないでしょう。
３０％確保できればこれをやってみてはどうだろうか？
この取引は７０％ぐらい PKI 普及しなければ危険だね・・・
利便性とセキュリティは相反するものかもしれませんが利便性をよくしてもリスクを低くする技術や法律、常識などは改善できると思います。
しかし、利用者が不安なのは技術者が思っているセキュリティとは違うかもしれませんね。
最後に、思いつきで作成している文章であり読みにくい点があったと思いますが、何かの参考にしていただけると幸いです。
今後も微力ながら PKI 普及への貢献が出来ればと思います。