デジタル世界の身分証明証その３
ー情報基盤センターPKI プロジェクトー

1. はじめに

PKI のことをよく知らない人から聞かれることは、「今 PKI の『電子証明書』や『鍵』を発行してもらって何ができるのか？」ということです。確かに電子証明書を発行されたとして、どういう用途があるのかという疑問を持つのは普通のことだと思います。そこで今回は予定を少し変更[※1]して、PKI で何ができるのか？という事例を紹介したいと思います。

2. PKI の技術を使ってできること

PKI の技術を使ってできることは前回説明しましたように認証（本人確認)、完全性（デジタル署名)、機密性（データの暗号化）です[1]。今回はその 3 点について具体的に説明します。

2.1 Web サービスに対しての認証（本人確認)

センターでは、施設予約やスケジュール管理するためのグループウエア、物品発注システム、事務部 Web メールなどといった Web サービスに対しての認証（本人確認）に電子証明書を使ってアクセスするという試行サービスをセンター内部向けに実施しています。

ところで、それらの Web サービスには SSL-VPN を経由してアクセスしています。SSL-VPN とは前回の記事[2][3]で述べていますが、簡単にいうとアクセスポイントです。VPN といった仮想的な専用線に SSL という通信規約を使っており、そのデータは暗号化されデータを見られる心配はありません。

なお、本センター図書館電子化部門では同じく SSL-VPN(PKI プロジェクトとは別製品)を経由して文献検索サービス（FELIX）や学内専用ページを閲覧できるサービスを試行しています（本冊子「ECCS アカウントによる学内 Web サービスのオフキャンパス利用サービス拡大のお知らせ」参照)。学内にある SSL-VPN を経由することにより自宅からでも FELIX を利用したり学内専用ページを閲覧したりすることができます。図１は自宅から学内専用ページの「教職員のみなさまへ」を閲覧している状態です。見た目は学内から閲覧している状態と変わりませんが、URL が通常の http://www.adm.u-tokyo.ac.jp/gakunai/index_j.html ではなく、SSL-VPN を経由するため https://sslvpn.ecc.u-tokyo.ac.jp/gakunai/,DanaInfo=www.adm.u-tokyo.ac.jp,SSO=U+index_j.html となっています（図 1)。認証(本人確認)は PKI ではなく、教育用計算機システム(ECCS)のユーザネーム（ID）とパスワードですが、今後 PKI 認証基盤が整備された場合には PKI を活用することも視野に入れています[2]。

---

1 前回の記事では情報基盤センターの電子証明書の発行・運用体制を説明しますと書きましたが、上記の理由により、次回以降の説明となります。ただし、PKI についてホットな話題があればそちらを優先します。

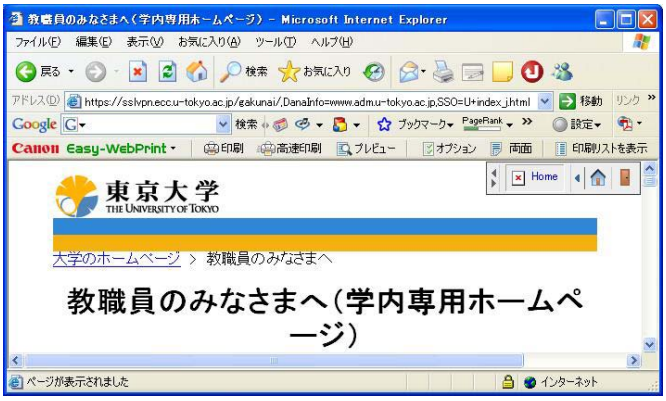

図１ SSL-VPN を経由して学内専用ページを閲覧

2.2 電子メールの暗号化（機密性）およびデジタル署名（完全性）

大学の業務で作成される文書には機密性の高いものが多数あります。例えば、入試関連、教職員の人事情報、成績関連、発表前の研究論文などです。そしてそれらの文書は電子メールという通信手段で関係者とやり取りする場合があるようです。しかし、電子メールは暗号化されていない文書を送ると盗聴されるという危険性を孕んでいます。だからといってあらゆる文書が盗聴されているとは思えませんが、悪意のある者が何らかの方法で電子メールを盗聴することはできるでしょう。PKI はそういった脅威に対抗することができます。ここで Microsoft(R) Outlook Express を例に電子メールを暗号化して送信する方法を紹介します。ただし、話の本筋から外れるのでここでは詳細な説明はしませんが、初めて暗号化メール（S/MIME）を送信する場合は事前に設定が必要です。さらに付け加えますと今回紹介した方法は、まずご自身に電子証明書が発行されていないと実践できません。また、相手先の電子メールソフトが暗号化メール（S/MIME）に対応していることが前提です。その点をご理解のうえお読みください。

さて、暗号化メール（S/MIME）を送信することは非常に簡単です。まずは Outlook Express を起動して、メールの作成をクリックします。次にツール→暗号化という順番にメニューを選択してください（図 2）。あとは送信ボタンをクリックするだけです。

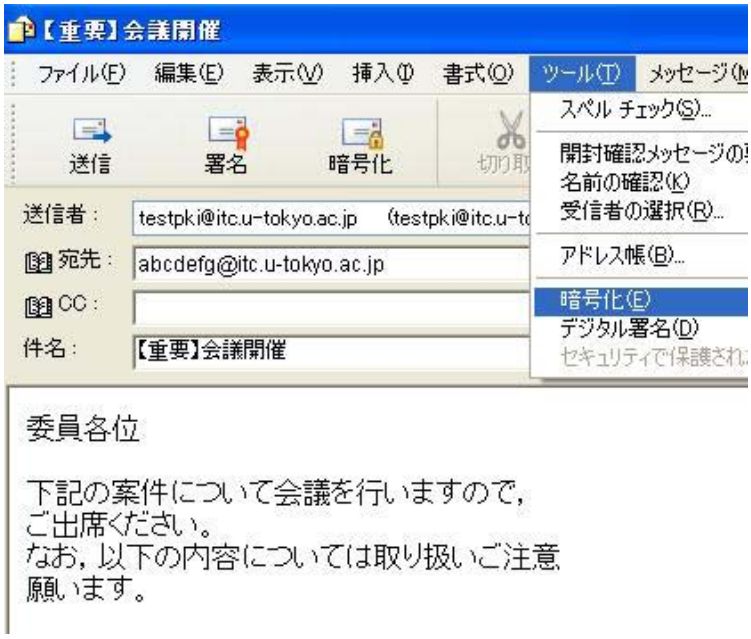

図２　暗号化＋デジタル署名付きの電子メールを送信

なお、通常は暗号化に加えデジタル署名も付与します。デジタル署名とは実社会でいう押印にあたるものです。そうすることによって相手方には「暗号化+デジタル署名」された電子メールが届くことになります。デジタル署名を付与するためには、図2の「暗号化」の下にあります「デジタル署名」をクリックするだけです。

それではメール本文作成中の画面を見てみましょう（図 3)。画面右上をご覧いただくと赤いリボンみたいなものがありますが、これがデジタル署名が付与された状態で、その下にある青い鍵みたいなものが暗号化されている状態を示します。あとは送信をクリックするだけです。正確には電子メールを送信したときの通信が暗号化されていることになります。

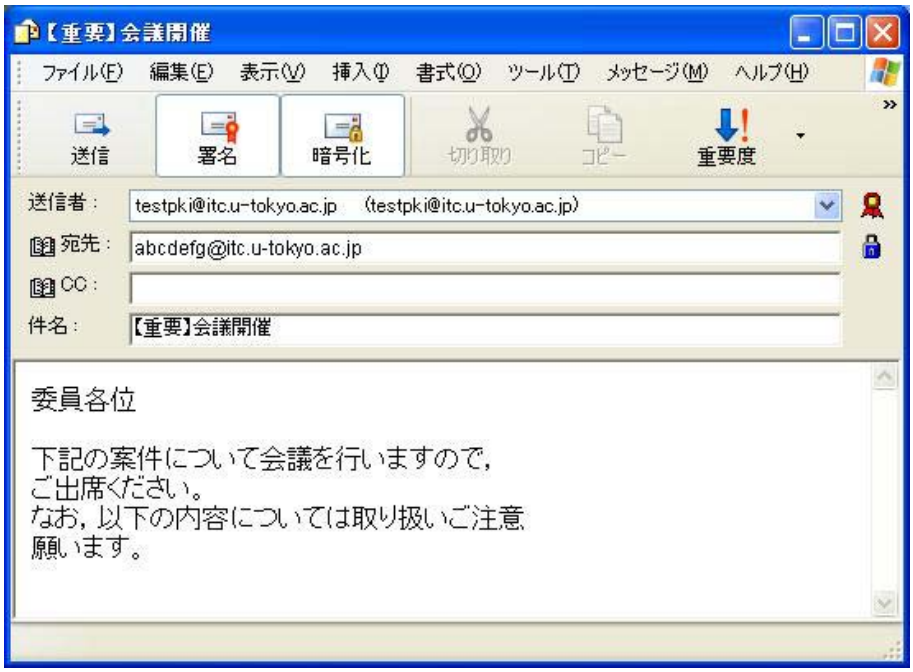

図3　デジタル署名と暗号化を選択した状態

図4　図3の画面を拡大

情報基盤センターで動作確認をしている暗号・電子署名対応メールソフトは、Windows 版では Outlook Express, Thunderbird, Shuriken Pro4, Becky!で、Macintosh 版では Mail と Thunderbird です。その他では動作確認はしていませんが、秀丸メールと Winbiff（ともに Windows 版）についても暗号化・電子署名に対応しているそうです。

3. おわりに

今回紹介した PKI の技術を応用して、例えば「出張先からメールが見たい」、「学生の成績を自宅から入力したい」、そのほか「こういうことをしたいけど PKI の技術を使って実現できますか」といったご要望がありましたら PKI プロジェクトの事務を担当しているアプリケ

ーション支援係（pki-request@itc.u-tokyo.ac.jp,http://www.pki.itc.u-tokyo.ac.jp/）までご連絡ください。実現に向けてご協力できれば幸いです。

参考資料：

[1] Digital Life Vol.7、http://www.pki.itc.u-tokyo.ac.jp/pdoc/digital_life/DL_V7_pp41-47.pdf
[2] ECCS アカウント認証による附属図書館 FELIX サービスの学外利用、Digital Life Vol.7 pp.13-14、http://www.itc.u-tokyo.ac.jp/DigitalLife/Vol7/Digital_Life_Vol.7.pdf
[3] Digital Life Vol.7、http://www.pki.itc.u-tokyo.ac.jp/pdoc/digital_life/DL_V7_pp38-40.pdf

（大島大輔）