2006.1.19

タイムビジネスに関する
欧州動向調査報告書
（英国、ハンガリー、スロバキア）

平成１８年1月

タイムビジネス推進協議会

はじめに

昨今の情報通信技術の急速な進展と共に、地球規模で流通する電子的情報を縦横無尽に活用できる、高度情報通信ネットワークの構築は既に現実のものとなりつつあります。また、2005 年 12 月には、政府から新たな IT 戦略である「IT 新改革戦略」の素案が提示され、更にこの流れは加速されることが期待されております。

民間分野における電子商取引、行政分野における電子政府・電子自治体を実現・推進することは、大きな価値を生み出すことは間違いありませんが、同時に、活用される電子データの特性を利用した「不正行為」や「システム障害」等に関するリスクも大きくなり、「電子データの原本性確保」は避けることのできない重要なテーマになっております。

これらの状況を背景として、タイムビジネス推進協議会では、標準時配信サービスや時刻認証サービスといった、タイムスタンプ技術を活用したビジネスを「タイムビジネス」と称し、その普及に向け民間事業者・大学・研究機関等の結束のもと、様々な活動を実施しております。

今回の海外調査は、当協議会の活動の一環であり、企画部会・調査研究分科会が中心となって、定期的に行っているものです。

前回のドイツ・ベルギー調査では、主にタイムスタンプに関する言及を含む「電子署名法」等の法制度を中心に関係部署への意見交換を行いましたが、今回は「タイムスタンプの具体的な利活用状況」をテーマとして、イギリス・ハンガリー・スロバキアの各国に対し訪問調査を実施しました。

日本国内では、2005 年 4 月施行されたいわゆる「e-文書法」によって、タイムスタンプの用途として、「企業等における法定保存文書の電子保存」がクローズアップされておりますが、これらの国々ではどのような場面での活用が考えられているか、どの程度普及しているか等が今回の中心的問題意識です。

今回の調査成果が、日本におけるタイムビジネス普及の一助になることを関係者一同、心から願っております。

最後に今回の調査企画に対して多大なご支援をいただいた nCipher 社の皆様に深く感謝の意を表したいと思います。

平成 18 年 1 月

タイムビジネス推進協議会

会長　大橋　正和

目 次

【関連資料】

・The large-scale archival storage of digital objects（The British Library）
・HP Trusted Audit: Solution Overview（HP：BRITISH GOVERNMENT）
・FELG Introduction（Fujitsu Europe Limited）
・The IT system of the Hungarian tax office（APEH）
・PKI- related technologies（SETCCE）

１．本調査の目的

タイムビジネス推進協議会では、国内外の利用動向調査や各種ガイドラインの整備等を行なっております。2004 年 3 月にドイツ調査団により、更なるタイムビジネスの制度的な枠組みを確立するために、タイムビジネスに関して法整備を行なっているドイツの実態の調査を行いました。また、引き続きタイムビジネスに関する欧州のサービス状況に対しヒアリング調査を行い、英国、東欧でタイムビジネスの動きが活発になっているとの状況がわかりました。

今回の調査目的は、英国、東欧（ハンガリー、スロバキア）の主要サービス事業者や政府機関への調査訪問を行い、ビジネスが展開されている状況調査をすることとしました。

２．調査スケジュール

11 月 27 日（日）　出国：結団式　成田空港発～ロンドン着

11 月 28 日（月）　THE BRITISH　LIBRARY、
HP　BRITISH GOVERNMENT　訪問

11 月 29 日（火）　FUJITSU EUROPE LIMITED 訪問

11 月 30 日（水）　HUNGARIAN TAX AND FINANCIAL CONTROL ADMINISTRATION、
MAV INFORMATIKA Ltd.
DNS Hungary Ltd.　訪問

12 月 1 日（木）　Viasec、Ministry of Defense、National Measurement Institutio 訪問

12 月 2 日（金）　SETCCE 訪問

12 月 3 日（土）　まとめ　帰国の途へ　ウィーン空港発 ⇒ ロンドン空港経由

12 月 4 日（日）　帰国：成田空港着

３．参加メンバー

(順不同・敬称略)

団　長	大橋　正和	中央大学総合政策学部長　総合政策学部教授・工学博士
副団長	三谷　慶一郎	株式会社 NTT データ経営研究所 情報戦略コンサルティング本部長　エグゼクティブコンサルタント
	清松　哲郎	株式会社東大総研　理事
	内藤　隆光	アマノタイムビジネス株式会社　代表取締役　社長
	石川　昭一	株式会社ＰＦＵ　プロダクト本部 イメージビジネス営業統括部タイムスタンプビジネス推進部 部長（兼）ソフトウェア開発部担当部長
	廣瀬　智康	丸文株式会社　情報機器部　情報通信課　主任
	林　誠一郎	株式会社ＮＴＴデータ　ビジネス開発事業本部 セキュリティビジネスユニット エグゼクティブ・セキュリティマネージャ
	井山　泰裕	株式会社ＮＴＴデータ　ビジネスソリューション事業本部 セキュリティサービスユニット　セキュリティビジネス担当
	伊藤　大輔	インターネットマルチフィード株式会社　技術部　担当課長代理
	本田　雅裕	株式会社エイベック　代表取締役
	小野　諭	工学院大学　技術者能力開発センター（CPD センター）　教授
	石垣　陽	セコム株式会社　IS 研究所　研究員
	倉田　道夫	財団法人デジタルコンテンツ協会　企画・推進本部 流通環境整備部　研究主幹
事務局	刑部　正敏	財団法人テレコム先端技術研究支援センター 研究企画部　調査役

４．総括報告

４．１　調査各国の利用状況

ここでは、調査した英国、ハンガリー、スロバキア、スロベニアの各国の利用状況についてまとめることとする。

４．１．１　英国

英国におけるタイムスタンプの利用状況について、大英図書館（The British Library）の利用、HP 社と nCipher 社が推進している英国外務省システムについての情報が得られた。

大英図書館では、書籍・出版物の収集・保存を行っており、保存に関しては永久保存である。通常の紙の出版物については、これまですべて大英図書館が蔵書とした日の日付入り蔵書印を付与している。そのため、蔵書印の日付におけるその出版物の存在証明として大英図書館の権威が広く認知されている。しかし、インターネットが普及した今日では、紙として印刷されずにインターネットで公開・出版された出版物が増大している。これらの紙でない出版物つまり電子出版文書に対応するためのプロジェクトが進行中である。これまで大英図書館が、維持してきた従来の出版物の存在証明における権威を維持し、今後増大する電子出版文書においてもその存在証明における権威を確保するためのタイムスタンプ付与である。大英図書館では、電子文書の真正性、完全性の確保を目指し、真正性確保のためのタイムスタンプである。電子データの形式に拘らずそのまま保存し、日本で電子文書の保存で同時に議論される見読性は別の課題として課題を分離している。また、蔵書印の日付を大英図書館が自らの責任で保障しているように、タイムスタンプの時刻の権威についても特に外に求めないという独自の立場を取っている。

英国外務省システムは、英国のセキュリティ関連の規制である CESG Memo 22 を踏まえたシステムである。この Memo 22 の規制では、システムログを 7 年間保存することを定めており、企業等のアカウンタビリティ確保のために、記録の保存を厳格化している米国 SOX 法、金融関連企業向けの新 BIS 規制（Basel II）等の一連のトレンドである。これはまたデジタルフォレンジックの証拠性確保の流れでもあり、保存の厳格化、証拠性の確実化のためにタイムスタンプを応用している。これは単なる一つの実装されたシステムというのではなく、アカウンタビリティ確保のトレンドを背景に今後の普及を見越して推進されているプロジェクトである。

４．１．２　ハンガリー

ハンガリーでは、国税庁が税の電子申告の証拠性確保のためのタイムスタンプの応用の他、IT 化推進、電子政府推進の状況とそれに関係する電子署名関連およびタイムスタ

ンプの状況のヒアリングを行った。

ハンガリーに限らずEU各国は1999年のEU電子署名指令に則った制度となっており、タイムスタンプは電子署名の機能を補完・補強するものとして理解され、位置づけられている。ハンガリーの電子署名法において、CA業務にタイムスタンプサービスは義務付けられておらず、CAの業務のオプションである。しかし現実には4つ存在する電子署名法準拠のCAはそれぞれタイムスタンプサービスを行っている。このことが表すようにハンガリーでは、電子署名とタイムスタンプは切り離せない関係であり、ヒアリングからも一般にはそのことが理論としてではなくむしろアプリオリにそう認識されているとも受け取れた。

ハンガリー国税庁の税電子申告のタイムスタンプ利用は、この電子署名とタイムスタンプが密接に関係する流れとは若干異なり、税の電子申告の授受の信頼性を向上させて問題の発生を軽減させようとするものである。行政へ電子申告された時刻証明のために民間にタイムスタンプの付与を義務付けているというものではない。タイムスタンプ付与によって税の電子申告の授受の時刻証明を行うことで、申告の時期を明らかにして申告に関して発生し得る問題を未然に防ごうというもので、タイムスタンプの時刻証明能力・証拠性向上の応用である。

ハンガリーでは、電子政府や電子取引などのIT化推進に熱心である。ハンガリー他の東欧諸国のEU加盟は、2004年5月であるが2001年にはEU電子署名指令を睨みさらに厳しい内容を盛り込んだ電子署名法を成立させた。まず厳しくしたほうが、早く課題を洗い出すことができ、洗い出した課題の解決を図るとともに法律は後で見直しをすればよいという考えに基づいている。関連法律・規則の整備を行い、熱心にIT化を推進している。これは、単に国内のIT化を目指しているというより、IT産業のコストの大半を占める労働コストにおいて自国の安い労働力を背景に、EU加盟国全体を市場として自国のIT産業の発展を期待している。しかし、EU加盟国といえどもEU全体の法体系が存在するわけではなく、EU加盟各国は自国の国内法に従っている。EU指令が、成立するとEU加盟国はそのEU指令に定められた期限内に対応した国内法の整備が義務付けられている。EU指令は、各国が実現可能な枠組みを定めるに過ぎず、詳細内容は各国の立法に委ねられている。このようなEUの制度の中で、ハンガリーに限らず2004年5月にEUに新規参加した東欧各国は、EU加盟諸国へ自国IT産業の進出を期待してIT関連の国内法をより厳しい内容にしているようにも見受けられる。ハンガリーのCAはセキュリティに非常に厳しいドイツの国内銀行へ売り込みを行いっている。なお、ハンガリーのタイムスタンプの価格は、大量に利用する場合にスタンプ当たり約1円（2フォリント）である。

2002年EU電子インボイス指令に基づき、ハンガリーでも2004年5月からEU加盟各国間との取引のインボイスの電子保管が可能となった。電子インボイス化も進んできているが厳しいハンガリー国内法では費用対効果が難しく普及には至っていないようで

ある。

４．１．３　スロバキア

スロバキアでは、Viasec 社、スロバキア技術大学の教授、タイムスタンプユーザーである国防省、タイムオーソリティである国立測量研究所等の関係メンバーが一堂に会した場においてヒアリングを行った。スロバキアは、ハンガリーと同様に 2004 年 5 月に EU に新規加盟した東欧諸国であり、ハンガリーの状況に非常に似通っている。

スロバキアは、2002 年に電子署名法を成立させた。ハンガリー同様に大変厳しい内容の法律となっている。電子署名法の中で民間でのタイムスタンプの応用、行政との遣り取りでのタイムスタンプの応用についての概要が述べられている。電子署名法が定める電子署名は、EU 電子署名指令に準じて 3 つのレベルがあるが最も厳格な適格電子署名の鍵はスマートカード等のセキュアなメディアに保管されなければならないとされている。

スロバキアの電子政府のポータルサイトにおいて、実質的にサーバが受け取りに電子署名を付与しているが、現在の電子署名法では個人にのみ証明書が発行されるために、サーバが付与する電子署名は電子署名法での電子署名として認められない。彼らは、それを一つの電子署名法の課題として捉えており、電子署名法の見直しでの議論する方針である。

スロバキアには電子署名法で認定された CA が、3 社ありその 2 社はタイムスタンプも供給している。それ以外に認定されていない CA が 5 社ある。

電子署名とタイムスタンプが、スロバキア国防省のシステムに利用されている。国防関係で従来の郵便に代わり、便利で速い電子メールの活用が検討されて、電子署名とタイムスタンプを付与する電子メールを利用するようになった。国防関連では、「誰が」と「何時」が特に重要であり、成りすましの対策および順序性を保障できることは重要である。電子署名とタイムスタンプによって電子メールを国防という非常にセンシティブな分野での応用を可能にしている。この流れは、一国にとどまらず NATO という範囲で電子署名およびタイムスタンプ付の電子メールの推進および標準化が進められている。

４．１．４　スロベニア（スロバキアにてヒアリング）

スロバキアにてスロベニアの SETCCE 社のヒアリングを行った。SETCCE 社は、スロベニア国立の研究所から PKI 開発部分が切り出されて設立された企業である。民間というより国が設立した企業であり、PKI 関連製品を開発・供給してその普及を図るために設立された。

スロベニアは、ハンガリーおよびスロバキアと同様に 2004 年に EU に加盟し、状況も似通っている。スロベニアでは人口約 200 万人の 10%が電子署名証明書を持つことが表すように、IT 化あるいは PKI の普及は非常に進んでいるといえよう。2000 年に電子署名法が制定されて、現在 4 つの認定 CA がある。そのうちの 2 つの CA が、タイムスタ

ンプサービスを行っている。

SETCCE 社は、PKI およびタイムスタンプ応用のライブラリやワークフローシステム、請求書発行システム、保管システムを開発・供給している。個別の SI は行わずに、パッケージ販売で市場はスロベニア国内にとどまらず EU 全体を狙っているものと思われる。

４．２　全体状況のまとめ

今回の海外調査は、結果的に EU 加盟の 4 カ国の調査となった。英国は、1973 年に EU（当時 EC）に加盟したが貨幣統合は行わず、他の EU 加盟国とは一定の距離を保っている。東欧の 3 カ国は、2004 年 5 月に新規に EU に加盟した国である。EU 加盟各国といってもそれぞれの立場は異なっている。

今回調査した各国の基礎統計と状況を簡単にまとめて下表に示す。

表 4-2-1　各国の基礎統計

国	英国	ハンガリー	スロバキア	スロベニア	日本（参考）
国土面積	24.3 万 km2	9.3 万 km2	4.9 万 km2	2.3 万 km2	37.8 万 km2
人口	5,923 万人	1,009 万人	541 万人	199 万人	12,762 万人
GDP	21,259 億ドル（244 兆円）	803 億ユーロ（11 兆円）	722 億 9,000 万ドル (8.3 兆円)	261.7 億ユーロ (3.6 兆円)	498 兆円
GDP/人口	30,244 ドル（347 万円）	7,948 ユーロ（110 万円）	13,300 ドル（153 万円）	13,103 ユーロ(181 万円）	390 万円
EU 加盟年	1973 年	2004 年	2004 年	2004 年	―
電子署名法	2000 年	2002 年	2001 年	2000 年	2000 年
認定 CA	？	４局	3 局	４局	19 局（業務）
認定 TSA	？	４局（CA）	2 局（CA）	２局(CA)	2 局（独立）
主なタイムスタンプ応用例	電子文書アーカイブ	税の電子申告システム	国防省メールシステム	電子署名応用システム	電子文書管理システム

※参考：外国為替レート（1 ドル：114.7 円、１ユーロ：138.1 円）で試算

英国では、大英図書館が独立組織としての立場で権威ある従来の出版物の保存と同様に、今後重要性を持つ電子文書保存のシステムを構築している。タイムスタンプの技術を用いているが、時刻の権威を外に求めることをせず技術的な裏づけと大英図書館自身の権威に基づいて、蔵書印を押印するように存在証明のタイムスタンプを電子文書データに付与して保存することを行う。時刻の権威を他に求めて証明するのではなく、自分自身が権威として従来の書籍同様に存在証明を行うところが特徴的である。このような

応用は、従来から出版物の存在証明で権威を保持し続けている大英図書館であるからこそできる応用例である。

英国の他の応用で、システム記録の保存の証拠性向上にタイムスタンプを用いることは、各種データのデジタル化および処理の IT 化とアカウンタビリティを厳しく求めるこの頃の流れに則った動きである。この流れは世の中に拡大していくと思われ、IT 化していく中で証拠性確保にタイムスタンプが有効であることがはっきり認識されていることが窺える。

東欧の 3 カ国（ハンガリー、スロバキア、スロベニア）は、互いに非常に似通っており、似た状況を示している。タイムスタンプの認識は、1999 年 EU 電子署名指令の考えに基づいているために電子署名の機能の補完として自然と理解されている。従ってこれらの国のすべての TSA は、認定 CA の付加サービスとして運営されており、大半の認定 CA がタイムスタンプサービスを持っている。

これらの 3 カ国に共通していることは、EU に加盟以前に制定した電子署名法は 1999 年 EU 電子署名指令を意識し、かつチャレンジングな内容の自国法を制定している。これは 2000 年 EU 電子取引指令、2002 年 EU インボイス指令、2004 年 EU 電子調達指令というように IT 化の推進される EU 全体を見据えて、まず国内 IT 化を推進して、廉価な労働力を背景にして EU 全体を市場とした一つの自国の産業として IT 産業を育成しようしている様子が見受けられる。この力がこの東欧の 3 カ国の電子署名やタイムスタンプの推進を支えており、国の規模がさほど大きくなく小回りが効く点等が合わさって先進の西欧諸国に勝るとも劣らないほど PKI およびタイムスタンプが普及しているものと思われる。

具体的な応用例としては、ハンガリーの税の電子申告の授受にタイムスタンプを付与させるシステム、スロバキアの国防省での電子メールに電子署名およびタイムスタンプを付与するシステム等の例があり、タイムスタンプによる証拠性の向上・信頼性の向上がはっきり認識されていることを示している。

タイムビジネス推進協議会
企画部会・調査研究分科会主査
株式会社東大総研
清松哲郎

５．訪問機関・企業報告

５．１　The British Library　（ 大英図書館 ）（英国）

PhD. Sean Martin 氏

Dr. Peter Whibbeley,氏　　講演風景

● 訪問日時：2005 年 11 月 28 日（月）　10:00～12:15

● 場所：The British Library 会議室

● 対応者：PhD. Sean Martin 氏
（Head of Architecture and Development, The British Library）
Dr. Peter Whibbeley, Senior Research Scientist 氏
（Time, Frequency & Metro Group, National Physical Laboratory）

● 報告者：内藤　隆光（アマノタイムビジネス株式会社　代表取締役　社長）
廣瀬　智康（丸文株式会社　情報機器部　情報通信課　主任）

● ヒアリング内容

大英図書館は、大英博物館から 1997 年に独立した機関であり、英国内だけに限らず世界中の人文及び自然科学に関する書籍を収集しており、紙の書籍を蔵書として登録する際には一部の特例を除き大英図書館の年月日付スタンプを押印している。書籍の収集、保存、閲覧を主たる目的とし、一度蔵書となった文書は永久保存することが原則となっている。

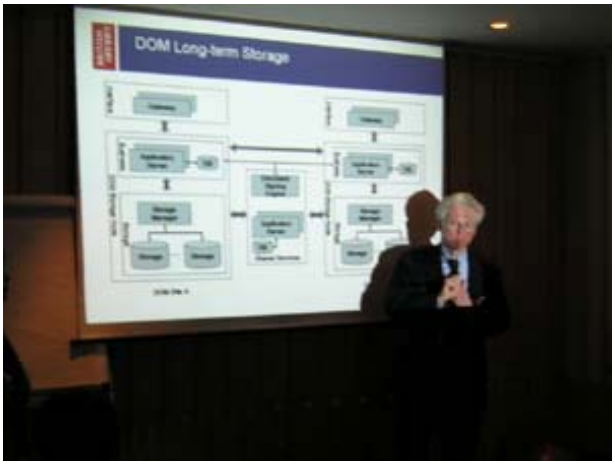
現在、大英図書館では、Digital Object Management(DOM) プログラムと呼ばれる電子文書保管のためのプロジェクトを 1 年半ほど前より組織化しており、紙の書籍同様、電子文書を永久保存することを目的として活動している。

電子文書保存管理システムを構築するにあたり以下の方針を基本としている。

- あらゆる種類の電子オブジェクトの永久保存
- アクセスコントロールによる閲覧者の制限
- 検索の簡易化
- 保存当時のアプリケーションによる閲覧を可能にする
- オリジナル文書と同じような感覚で閲覧できる工夫をする

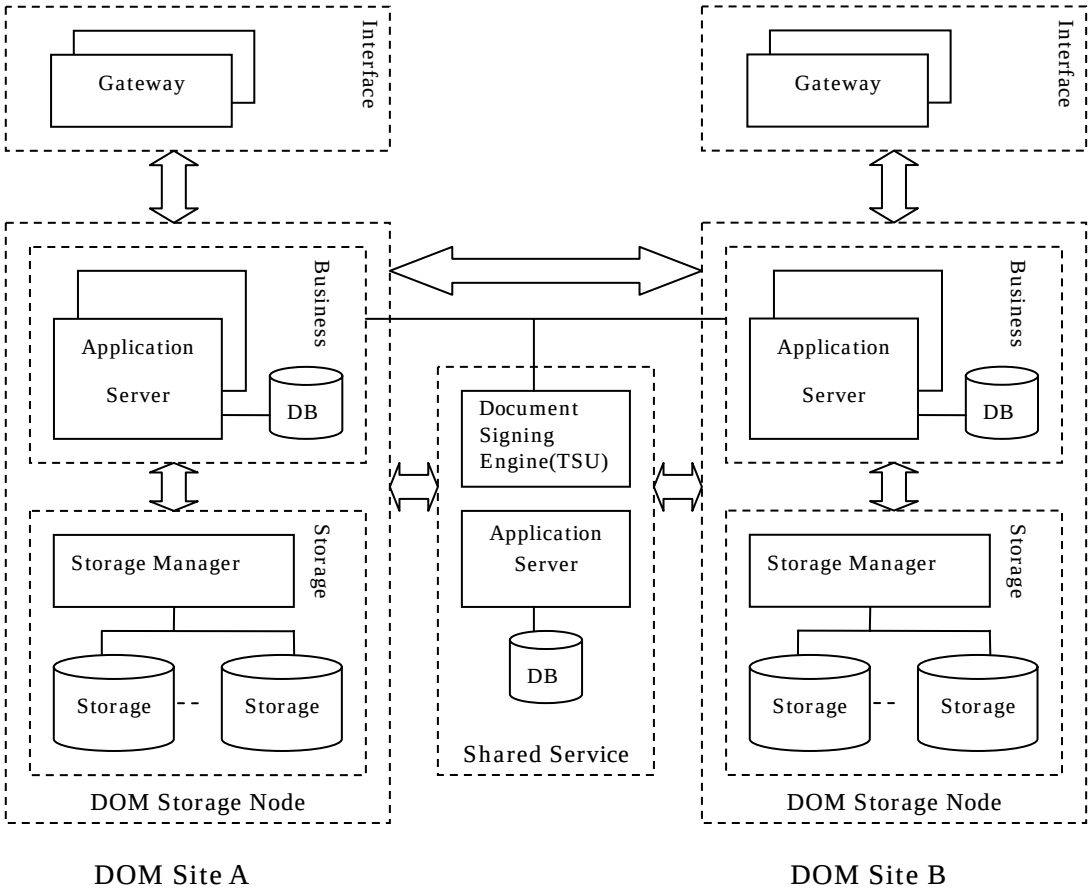
DOM プログラムを遂行している背景として、1911 年に制定された法律にて、英国内の出版社は紙書籍を出版した際には必ず複製物を大英図書館に提出するよう義務付けられていた（Legal Deposit と呼ばれている）が、2003 年 10 月の法律改正にて、電子化文書も同様にコピーを提出するよう義務付けられたことが挙げられ、これにより膨大なデータ量の保存が必要になってきた為である。 大英図書館では、2000 年以来、voluntary deposit (法規制以外の保管)を実施しており、現在約 2 テラバイトのデータが保管されている。また、蔵書の電子化を 1990 年初頭より実施しており、 約 20 テラバイトのデータが保存されている。また、7 億 5 千万ページの新聞、1800 年代後半からの音楽コレクション、雑誌等が保存され、音楽 CD については、年間 1 万 5 千枚（約 15 テラバイト）を保存している。また、Legal deposit (法的な保存)については、英国内の Web に保存する必要がある。

技術的側面からは、Authenticity（真正性）と Integrity（完全性）を基本コンセプトして掲げており、中でも Authenticity を重視している。紙書籍であれば、化学的な紙やインクの調査により発行年代を証明することが可能であるが、電子文書に対しては同様な調査は不可能であるため、タイムスタンプ技術を利用し、「いつ」保存されたものかを検証することを可能にしている。Integrity については、ハッシュ関数を利用し、改ざん検出により実現している。



【写真 5-1-1】The British Library の Martin 氏による説明風景

DOM 長期保存システム構成図は下図の通りとなっている。



【図 5-1-1】Digital Object Management(DOM)構成図

電子化文書保存 DB は災害時対応を重視し冗長構成となっており、プライマリ系は大英図書館本館に、セカンダリ系は約 200 マイル離れた別サイトにて運営されており、 それぞれが Document Signing Engine と呼ばれる nCipher 社タイムスタンプサーバ（2 台所有）からタイムスタンプを取得できる構成になっている。

大英図書館の紙書籍に押印されたスタンプには法的効力も有しており、幾つかの裁判において同スタンプの日付が裁判での法的証拠として使用された事例もある。（参照：Rhone-Poulenc. Source : 'Report of Patent, Design, and Trade Mark Cases', 1996 no. 4 p125 及び Viziball Ltd. Source : 'Report of Patent, Design, and Trade Mark Cases', 1988 no. 11 p213）

【写真 5-1-2】紙の出版物への押印

Ingest（収集）、Preservation（保存）、Access/Deliver（閲覧）の各過程において、Ingest と Deliver は非常に短期間の作業であり、Preservation は非常に長期間の作業となっている。Ingest はユーザーと大英図書館との関係、Deliver は大英図書館とユーザーとの関係であり、それぞれが PKI の技術で信頼性を実現している。Preservation については、紙書籍同様、大英図書館内で非常に長期（千年単位のイメージ）にわたる信頼の置ける保存が求められている。これをどのように実現していくかが当面の課題である。大英図書館の歴史から比べると電子認証局のような外部の民間企業の歴史は浅く、これらの外部民間企業の信頼は大英図書館にとって価値をもたらさないと考えており、将来的には大英図書館のプライベート認証局による運営を目指している。

● 質疑応答

Q： TSA 証明書はどこが発行しているのか？ またタイムスタンプの有効期限は？

A： 大英図書館は、現在 2 台の nCipher 社 DSE を所有しており、現在は TSA 証明書を nCipher 社から発行してもらっている。また、時刻ソースは英国における NTA である National Physical Laboratory から供給してもらうよう折衝中である。タイムスタンプの有効期限については出来るだけ強固な暗号を利用することにより長期保存に備えると共に、将来的に危殆化した場合には再署名することで対処する予定である。その再署名の周期については未決定である。

Q: 電子化コンテンツ自身にタイムスタンプも含むのか？また保存対象のファイル形式は特定されているのか？

A： DOM ID という証明番号により管理し、domid.dat（オリジナルのビットストリーム）と domid.sig（XML にて署名されたファイル）を別々に管理し、検証時に比較することになっている。保存対象ファイル形式は指定されておらず、様々なフォーマットで保存しており、将来的にアプリケーションに依存しないための保存手法に関してはまだ結論が出ていない。スキャンする場合には TIF 形式を利用している。

Q: 一般市民が大英図書館に電子化コンテンツの保存を依頼することは可能か？その場合、どのように著作者の認証を行うのか？

A： 将来的には、大英図書館で一般市民の電子化コンテンツの保存をするのは可能となる予定。認証については、PKI を利用し、「誰」から送られてきて「いつ」登録したのかを認証する。

Q： DOM プロジェクトに何名従事しているのか？　またタイムスタンプには？

A： 15 名、うち 2.5 名がタイムスタンプに従事している。数が少ないのは、現在 voluntary deposit（約 2 テラバイト、月々数千文書の保存）に関してだけタイムスタンプを利用しているため。2006 年 6 月に雑誌関連にも適応する予定である。

● 補足

会議終了後、時刻ソースに関して National Physical Laboratory（NPL）の Dr. Whibbeley 氏に今後の取組みを伺ったところ、The British Laboratory からはタイムスタンプユニット（DSE）に時刻配信・監査を行うマスタークロックを NPL に設置し、配信・監査サービスを提供することの可能性検討を依頼されているとのことであった。

ちなみに日本の認定制度で採用されている GPS コモンビューによる国家時刻標準機関（NTA）との追跡性確保の事例を話したところ大変興味をもたれていた。

【写真 5-1-3】The British Library 外観

【写真 5-1-4】The British Library ロビー

【写真 5-1-5】The British Library にて

５．２　HP：BRITISH GOVERNMENT　(英国)

● 訪問日時： 2005 年 11 月 28 日（月）　14:00～16:00

● 場所：HP 会議室

● 対応者：nCipher 社　Scott 氏（Director of Sales－Time Stamping Solutions）
Robert Ruttgen 氏（Territory Manager Eastern Europe）
（HP 社　Graham Stone 氏の代理）

● 報告者：石川　昭一（株式会社 PFU プロダクト本部イメージビジネス営業統括部
タイムスタンプビジネス推進部　部長（兼）ソフトウェア
開発部担当部長）
伊藤　大輔（インターネットマルチフィード株式会社　技術部　担当課長
代理）

● ヒアリング内容：

(1) はじめに

英国において、HP が進めてきたタイムスタンプを利用したソリューションの紹介を行う。HP と nCipher が、過去２年間協力して開発を行ってきた、Trusted Audit Solution と呼ばれるソリューションである。まだ、市場に出していない新商品で、一カ月以内にリリース予定である。英国政府や大企業は、このソリューションが実施される事に対し強く関心を持っている。

(2) 背景について

本ソリューションは、CESG Memo 22 を初めとした各条件・法制度に対応できるような柔軟性のあるソリューションとして開発したものである。CESG とは、中央政府のセキュリティ関連の本部で、色な標準化の設定を進めている。memo 22 では、中央政府の色々な記録を 7 年間保持することが求められている。モニタリングも必要であり、Integrity（完全性）と Authenticity（真正性）のものを残すため、タイムスタンプテクノジーを使って保存を行っている。最初に中央政府が、このようなソリューションを活用する機関となっているが、他の省庁でも使われていくことになる。さらに、このソリューションは、他の大企業でも SOX 法、Basel、データプロテクション法に応じていくためにも役に立つ仕組みである。

(3) HP Trusted Audit Solution について

システムをモニタリングするソリューションであり、Man in Middle Attack や DoS、設計者の意図しないアクセスなどの脅威に対して検知・警報を行うシステム。各種データも改ざんができないように対策される。（費用は、数百万ポンド）

システムは、大別すると Client と Collector に分かれる。Client は、TCG などが導入された高信頼性クライアント（Trusted Client）で、その高信頼性クライアントに関する各種ログ情報が Collection Point（各国大使館など）に収集される。各 Collection Point を経由して、Central Collection Point へ集められ監視を行っている。

収集は遠隔地など、様々な環境の Client に対応可能であり、一方通行の通信でセキュアに実現される。これは英国外務省と、各国大使館を接続するようなシステムを想定している。集められたログに対しては、様々な脅威について検査・検知・警報などが逐一実施される。

(4) 本サービスにおけるタイムスタンプの利用範囲

高信頼性クライアントが、自己の各種ログをその生成された時刻も含めて有効であることを証明するために、各高信頼性クライアントでログを収集するたびにタイムスタンプが用いられる。（収集する間隔は任意。）

時間は、複数の TA より DS/NTP により配布される。TA から時刻を受けたサーバが、さらに他 Client/Server へと DS/NTP により時刻を配布する。これにより、システム全体の時刻の同一性を保たれる。

(5) その他

本システムでは、CA は特に定められていない。自前に構築することを想定していると思われるが、柔軟性のあるシステムという口調から既存の公開鍵基盤の利用も可能であると考えられる。

現在は、英国連邦・外務省を含めたシステムでの利用を想定しており、高信頼性クライアントの監査対象アプリケーションは全てである。

アプリケーションデータに直接タイムスタンプされるのではなく、高信頼性クライアントのシステムログだけである。

● 質疑応答(一部、前記と重複)

Q： もともと英国外務省での利用を想定しているとの話だが、具体的にはどのようなアプリケーションのログの取得を考えているのか？

A： このシステムは、すべてのイベントのログを取得する。外務省は、最初のユーザーとなる予定だが、結果的にはその外務省で利用しているアプリケーションすべてを含むことになる。

Q：　具体的なログのイメージが見えない。ログとはデータそのものなのか？

A：　それぞれ起こったイベントが収集される。侵入はどこから行われるのか分からないので、広範囲な収集が必要である。

Q：　取得し、保存・監査するのはデータベースのジャーナルログのことなのか？

A：　データベースを見ているアクション自体がログに入ってくる。データそのものではなく、データのアクションを見るものである。

Q：　送付されるデータとは、例えばメールの場合、メールそのものも対象なのか？

A：　そこまでモニタ可能かどうかは、分からない。高信頼性クライアントがどこまで求めているかにもよる。

Q：　開発は英国が行っているのか？

A：　開発は U.K.の HP が行っているが、システム化が終了すれば、利用は世界中のＨＰから行えるはずである。

Q：　CESG memo などのルールの話題が出たが、そのなかでタイムスタンプを使うと明記してあるものはあるか？

A：　Recommended になっているものはある。しかし義務づけられてはいない。

Q：　SOX 法との関わりはどうか？

A：　そういった法律などに対応するために HP が開発したソリューションである。

Q：　CA はどこから行われるのか？

A：　柔軟性のあるシステムなので特に規定していない。（まだ、決まっていない）

● 考察・所感

侵入やなりすましに対して監査を行うためには、システムログの真偽性や生成された時刻が正しいことを保証されたシステムでないといけない。その観点からログにタイムスタンプを行うということは非常に理にかなっており、セキュリティの高いシステム構築に大変有効なソリューションと思われる。

しかし、高信頼性クライアントそのものに手を入れる必要があることに加え、想定されるコストが数百万ポンドとのこともあり、本システムの導入には一定のハードルが存在すると思われる。やはりこのような形でのタイムスタンプの使われ方は、もともとのターゲットとされる政府系やセキュリティへの要求が高い大企業から始まっていくものと思われる。

５．３　Fujitsu Europe Limited　（ロンドン）

HIDETOSHI　FUKUDA 氏

ＴＢＦメンバー

● 訪問日程：2005 年 11 月 29 日（火） 14:00～16:00

● 場所：Fujitsu Europe Limited（ロンドン事業所）

● 対応者：HIDETOSHI　FUKUDA 氏（General Manager）
AKIO　SUZUKI 氏（Technical Manager）
KEN H. ASHIDA 氏（Director）

● 報告者：林　誠一郎（株式会社ＮＴＴデータ　ビジネス開発事業本部
セキュリティビジネスユニット
エグゼクティブ・セキュリティマネージャ）
井山　泰裕（株式会社ＮＴＴデータ　ビジネスソリューション事業本部
セキュリティサービスユニット　セキュリティビジネス
担当）

● ヒアリング内容

(1) Fujitsu Europe Limited について

富士通ヨーロッパ Ltd のロンドン事業所は、イメージングデバイスや生体認証機器の拡販を目的として 2005 年 6 月 20 日に開設された。

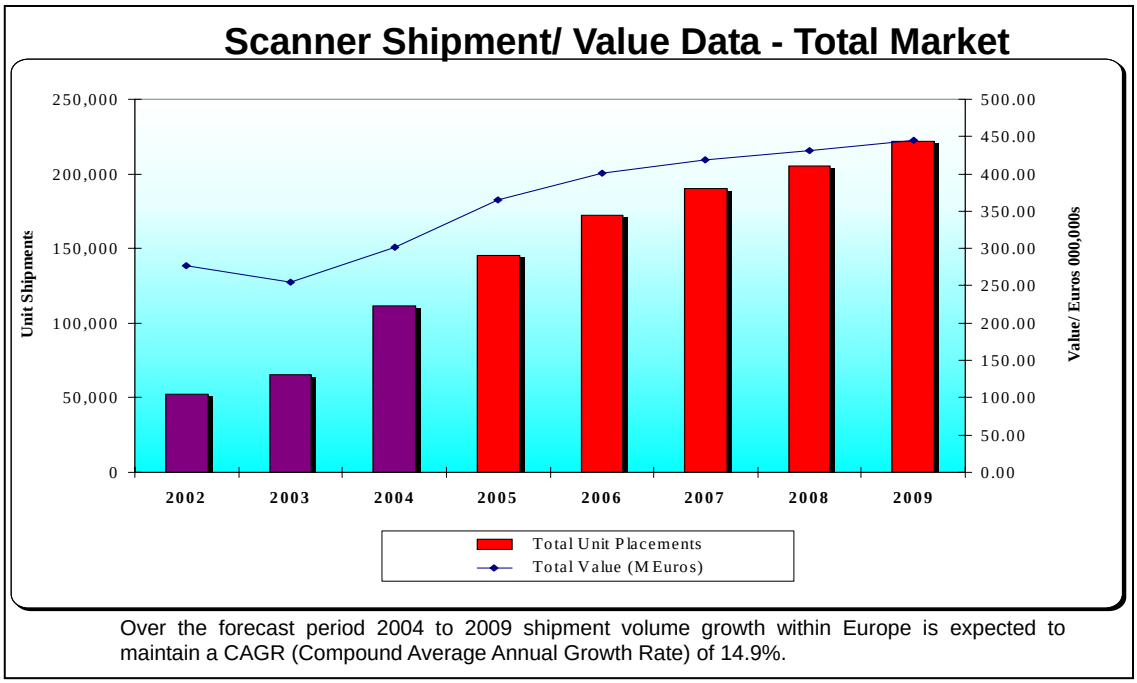
ハードウェア、アプリケーションソフト、SIer などのパートナーのための製品展示や試験スペースとしても利用されている。

(2) 生体認証機器について

生体認証機器は、指紋と静脈の 2 種類を扱っている。ヨーロッパにおいては、生体認証の導入があまり進んでいないため、啓蒙活動を中心に行なっている。特に英国の金融機関は、あまり導入に活発ではない。日本では、ATM の生体認証が広がってきているが、ヨーロッパでは ATM の大半が屋外に設置されており、生体認証機器の認識率や耐久性に対する障害となっている。また、生体認証に対する社会的責任をどのように扱うのかという課題もある。

(3) スキャナ機器について

スキャナ機器は、需要が右肩上がりで伸びており、売上も年率 15%の成長を続けている。ヨーロッパにおいてスキャナは、帳票や小切手の読み取りのために多く利用されている。また、病院での処方箋読み取り用としても普及しており、小規模の診療所でもスキャナは利用されている。イメージデータは、OCR で必要データを抽出し、業務処理に使うことが主たる利用方法で、日本の e-文書法のような保管に関する法律はないため、原本は紙のまま保管されることが多い。そのため、OCR に適した解像度（300dpi）、グレースケールでのスキャン機能を有した製品が主力となっており、売れ筋は 1000 ドル前後の製品である。



（Source： Infosource June 2005）

【図 5-3-1】 European Market Overview Source（出典：FELG ﾌﾟﾚｾﾞﾝﾃｰｼｮﾝ資料）

(4) タイムスタンプについて

現在、富士通ヨーロッパ Ltd.では、タイムスタンプや電子署名のオプション製品の取り扱いはしていない。

【写真 5-3-1】生体認証機器デモ説明風景

【写真 5-3-2】スキャナ機器デモ説明風景

【写真 5-3-3】Fujitsu Europe Limited 会議室にて

５．４　HUNGARIAN TAX AND FINANNCIAL CONTROL ADMINISTRATION （APEH）　(ハンガリー)

意見交換風景

Dr. Ivan FUTO **氏**

● 訪問日時：2005 年 11 月 30 日（水）　9:00～11:20

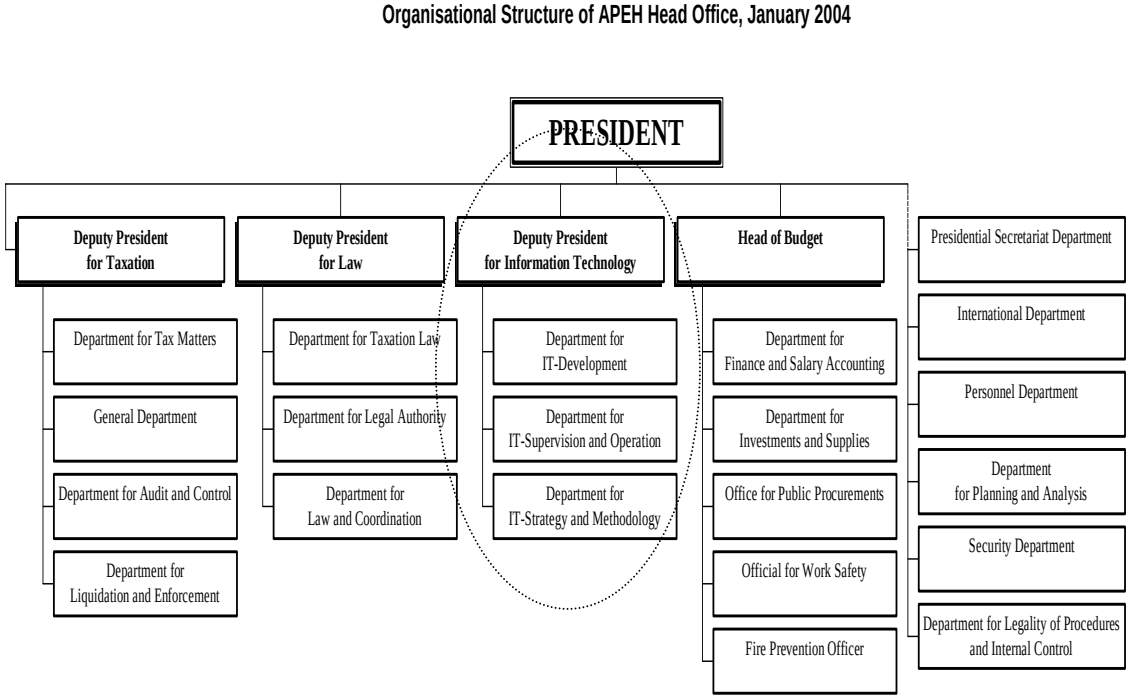
● 場　所：HUNGARIAN TAX AND FINANNCIAL CONTROL ADMINISTRATION 会議室

● 対応者：Dr. Ivan FUTO 氏 (Vice president of APEH)
Nagy ZOLTAN 氏 (PILLER 社)

● 報告者：小野　諭　（工学院大学　技術者能力開発センター（CPD センター）教授）
清松　哲郎（株式会社東大総研　理事）

● 組織概要

ハンガリー共和国は、2005 年現在人口 1,009 万人、国土面積は日本の約 4 分の 1 である。GDP は 803 億ユーロ（2004 年）、2004 年に EU に加盟した。訪問した APEH は、ハンガリーの国レベルの税務を扱う庁であり、Dr. Ivan FUTO 氏 はその税務庁の IT 関連を纏める Vice President である。IT 関連では、Development Dep., Operation Dep., IT Strategy & Technology Dep.の 3 つの部がある。PILLER 社は、国税庁の IT 部分を担う子会社である。



【図 5-4-1】Organisational Structure of APEH Head Office, January2004

● ヒアリング内容

税務庁の組織は、2004 年 1 月に大きく組織変更されて現状の組織になった。税務関連 IT システムは、ハンガリーでもっとも複雑で巨大なシステムである。システムは、国家レベルとカウンティレベルの 2 層からなる。
システムの規模はおよそ次の通りである。

- workstation 12,000 台以上
- server 200 台以上
- router 等　450 台以上
- 800 名の IT スペシャリスト

2005 年 11 月に紙で行う手続きは､電子的に行うことを包括的に認める法律が成立した。この法律に基づき、2006 年には約 40,000 社の大企業が電子申告を行うことになる。さらに 2007 年には 1,200,000 社が電子申告による手続きを行う。ただし、電子署名は未適用である。

電子申告のシステムは、国税庁と企業でデータを遣り取りする共有ボックスを持ち、関連プログラムは Web からダウンロードして利用する。電子申告を行うためにダウンロ

ードされたプログラムは、国税庁の公開鍵(証明書)を持ち、申告データを暗号化して共有ボックスに格納する。国税庁では、共有ボックスに格納された申告データにタイムスタンプを付与すると同時に、タイムスタンプ付の受領証を共有ボックスに格納し、受領証が発行されたことを e-mail で申告者に通知する。

法的背景として、ハンガリーでは 2001 年に電子署名法が制定された。しかし、内容は厳しすぎるものであり、適格電子署名の環境は 2003 年まで揃わなかった。電子署名法の法律の周りに多くの法令が必要であり、e-Business 法など、その整備に時間が掛かった。紙文書をスキャンして電子化することは認められている。

認証局（CA）に関して電子署名法に技術・組織等が詳しく規定されており、厳しい認定がある。2005 年の改定で現実を鑑みて規定が若干緩くなった。現在ハンガリーでは、下記の 4 つの組織が CA サービスを行っている。

① ハンガリー（マジャール）テレコム
② マットインフォマティックス社
③ ネットロック社
④ ミクロセック社

タイムスタンプについて、電子署名法で電子署名・電子証明書とともに CA が持つべきタイムスタンプサービスについて規定している。電子署名法では、義務ではなくオプションであるが、4 つの CA ともタイムサービスを行っている。

タイムスタンプを付与している書類としては、電子的に申告された税の電子申告書および受取証以外にも、請求書の保存、証明書の発行について EU の規定に基づいて行っており、タイムスタンプを付与している。

● 質疑応答

Q： タイムスタンプはどのように規定されているか？電子署名とタイムスタンプの関係はどうなっているか？

A： タイムスタンプについては電子署名法で電子署名とともに CA が持つべきタイムスタンプサービスについて規定しているが、義務ではなくオプションである。しかし 4 つの CA ともタイムスタンプサービスを行っている。

Q： タイムスタンプを付与している書類は具体的にどのような書類か？

A： 電子的に申告された税の電子申告書およびその受取証、また請求書の保存、証明書の発行については EU の規定に基づいて行っており、タイムスタンプを付与している。

Q： 国税庁のサービス内容はどんなものがあるか？

A： ハンガリーは、2004 年 5 月に EU に加盟し、行政サービスにいろんな条件が課せている。たとえば、それぞれの国民に提供するサービスのうち多くのものは電子サービスにする必要がある。そのうち税に関するものは 4 つ、所得税、法人税、社会保険、消費税である。

国税庁がサービスする内容は、homepage, E-mail 定期的なメール、税金の確定申告などで、半分電子、すべて電子の 2 種類の申告方法がある。

電子的な確定申告は、電子署名するか、パスワードとユーザー名をいれて提出する。タイムスタンプを何度か使う。半分電子化された申告は、書類に対応したソフトを用いる。4 年前から 150 の書類とそのソフトがダウンロードできる。

ソフトをダウンロードして、そのソフトがデータを確認する。終わったら、それをプリントして国税庁に送る。各ページの出力は、2D バーコード化されている。これは、2D バーコードリーダにより読み込まれる。

国税庁では、これにより文書を OCR などで読まなくて良くなる。ハンガリーでは、4 つの組織が CA サービスを行っている。

Q： サービスの実績はどんなものか？

A： 2004 年の確定申告の 49%が、半分電子化されたシステムによって、行われている。法人税では、2005 年で 72%にもなっている。

100%電子申告の場合は、2002 年 10 月から一番大きな納税者 420 社に義務付けられた。これは、税金の 35%になっている。2005 年 1 月からは規模の上位 10000 社にする。義務づけられる。これは、納税額全体の 64%に達する。

この申告方法では、3 枚のチップのカードとリーダをユーザーに提供する。国税庁は、登録、CA もやっている、2004 年まではタイムスタンプもこの会社がやっている。2004 年からは外でやっている。今年は、電子申告の会社は 40 万になる。

2005 年 4 月から、希望する企業、人がいわゆる政府 e-safegate を通していろんな書類を出すことができる。パスワード、ユーザー名をもらって登録する。この登録は、内務省オフィスで行われ、現在、250 ユーザーである。

国税庁は、登録された人の中で、その会社の代表としてサインする権限があるかをチェックしている。また、改ざんを防止するため、別の会社に頼んで、タイムスタンプをもらっている。登録された企業について、確定申告、その前、さらにその前の申告を見ることができる。

Q： 法律・規制関連の状況はどのようになっているか？

A： 2005 年 11 月から、政府の事業の新しい法律ができた。その法律に書かれているのは、紙の処理でできることはコンピュータでもできるということである。ただし、現在は、対応するインフラはないので、みな、紙の書類を出す許可をもらっている。国税庁も電子化した書類のインフラを持たないので、多くの書類を紙で提出してもらっている。

電子証明は、国でひきうけるのは非常にむずかしい。国の審査をうけないと活動できない、こういう機関はまだない。国会が税制を変えることにとりくんでいる。一番大きな納税者（会社）4 万は、電子的に確定申告を行うことになる。

一年たって、2007 年からは、120 万の企業が電子的な確定申告を義務付けられる。来年からは紙による申告はチョイスできなくなる予定（12 月 12 日に国会で決める予定）。書類に電子署名はない。サインにはメールボックスシステムを利用している。

Q： 国税庁のシステムでいうメールボックスとはどのようなものか？

A： 各カスタマ、内務省に登録した人は、メールボックスをもらう。これは、その会社以外誰もみることができない。納税者と国との通信は、このメールボックスを経由して行う。長い時間かかる書類の記入は、国税庁提供ソフトを使いオフラインで行われる。確定申告には 2 時間以上かかる。もちろん、オンラインのコミュニケーションも必要で、そのサービスは、内務省が提供する。

Q： メールボックスはどのように動作するか？

A： クライアントソフトをダウンロードする。このソフトが、国税庁のパブリックキーも入っており、外からの情報をパブリックキーで暗号化する。第三者からタイムスタンプをもらって、このメールボックスを経由して文書を送る。データセキュリティの関係で、暗号化されたメールしか入っていない。

納税者が、メールボックスにメールを入れると、メインシステムが国税庁のあるオフィスに、それを転送する。国税庁は、メールボックスを経由して“引き受けた”というメッセージをお返答する。メールボックスにメッセージが書き込まれると“メールボックスを見るように”というメールが納税者宛に送られて来る。1 週間以内にメールを見ないと、封筒で同じ書類を配送する。

会社が、提出する文書にはいろんな署名が必要である。文章を表示して“それにサインするように”と指示される。

カスタマが、登録した時にふたつのキーをもらう。パブリックキーは、メールボックスを経由して国税庁がカスタマにメッセージを出すときに、このキーを使用

する。カスタマは、プライベートキーで解読する。このサービスは 5 月から実施している。

Q： 電子署名とタイムスタンプの関係はどのようになっているか？

A： 電子署名では、タイムスタンプを付与できる、ただし、義務ではない。タイムスタンプだけを使うカスタマはほとんどいない。ただし、税務で 1 箇所だけは、タイムスタンプだけを使っている。申告書類の受取証明書で、タイムスタンプが付与されている。書類を“いつ”出したかを証明してもらうためである。ハンガリーでは、納税者は、これを 5 年間保存する義務がある。

ハンガリーでは、タイムスタンププロバイダは、同時に CA でもある。ハンガリーは EU に法律に基づく。電子化された請求書。いろんな証明書を出すときにも、電子署名やタイムスタンプを付与する。これは、EU 各国で使える。

文書保存のしかたも法律になっている。CA，TS，保存の 3 つのサービスは、今のところ一緒にやる事業者が多い。長期保存（10 年間）の場合、1 年ごとにタイムスタンプを付与しなおす。

タイムスタンプは、インターネット経由で発行する。ユーザーはどこにいるか関係ない。ハンガリーは、人口 1000 万人だが、EU には 3 億人いる。ハンガリーのものは、他の国でも理論的に認められなければならない。

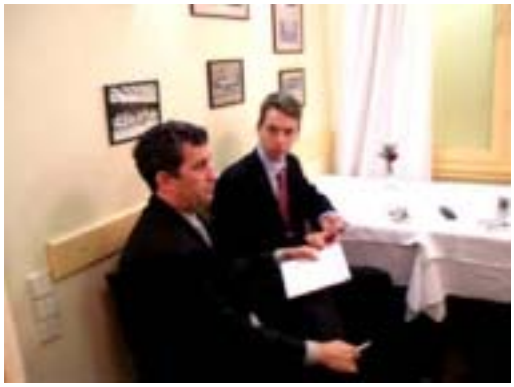
それぞれの国の法律は、EU 指令をもとに作られている。ただし、インプリメントは、指令には強制力がないため国ごとにかなり違っている。1999 指令では、2001 年までに対応する法律をつくることになっていた。EU 指令は最低限のことを規定し、ドイツはそれより厳しい。

ドイツでタイムスタンプをサービスするには、ドイツの法律に適合する必要がある。HU の会社で、HU とドイツの規制を満たすサービスをする。HU とドイツの生活水準に差があるため、HU のほうがずっと安くタイムスタンプをサービスできる。

ドイツのサービスでは、EAL-5 を要求する。FIPS 準拠の HSM が必須である。（レベルは不明）HU では、Utimaco や IBM の HSM を使っている。価格は数にもよるが、2 フォリント（1 円ちょっと）である。

【写真 5-4-2】HUNGARIAN TAX AND FINANNCIAL CONTROL ADMINISTRATION 会議室にて

５．５　MAV INFORMATIKA Ltd.(ハンガリー)



Robert Kisteleki 氏

意見交換風景

● 訪問日時：2005 年 11 月 30 日(水)　12:00～13:45

● 場所：レストラン Biarritz

● 対応者：Robert Kisteleki 氏（Director）

● 報告者：伊藤　大輔（インターネットマルチフィード株式会社　技術部担当課長代理）
本田　雅裕（株式会社エイベック　代表取締役）

● ヒアリング内容：

(1) はじめに

ハンガリーにおけるタイムスタンプを利用したサービスの動向について、インフォマティクス社の Robert Kisteleki 氏から意見を得る機会を得たので、ここに報告する。

インフォマティクス社は、ハンガリー国内において、SI をはじめとした IT サービスを提供している企業である。PKI サービスも行っており、CA を行いながらタイムスタンプも提供している。電子署名に関する法律により、ハンガリー政府の認定を受けた 4 社のうちの 1 社である。

(2) ハンガリーにおける電子署名とタイムスタンプの動向

ハンガリーでは、電子署名が使える法律が制定されている。すなわち、2004 年 5 月からインボイスの電子化が認められ、企業間の全ての取引データを電子的に行うことが可能である。この電子インボイスには電子署名とタイムスタンプの付与が必要である。ただし、電子化は義務ではないので普及していないのが現状である。

しかし、2005 年 12 月に国との取引では電子署名が義務付けられた。この法律が、契機となって一般への普及の促進が期待されている。

それ以前は、企業の納税申告の電子化で電子署名が義務付けられていたが、これは例外的な利用である。ただ、国税庁が提供している電子署名システムは、使用が特殊なため、税金申告以外に使えないものである。一方、民間会社が手がける電子署名サービスは、汎用的なものである。そのため、電子署名を利用する企業は、国税庁向けとそれ以外向けと 2 種類を使い分けなければならない。

その煩雑さを解消し経費を削減するため、民間企業が提供するより広範囲に適用可能な電子署名サービスを、税金関係にも使えるようにして欲しいとの要望が上がっている。それに対してハンガリー政府内では、独自のタイムスタンプを作成しようとする動きもあるが、国内主要 4 社が反対している状況にある。

現在、e-政府に向けて国内の法整備が進んでおり、税金の確定申告以外でも様々な書類を電子化して提出できる方向に進んでいる。これらの文書には、電子署名とタイムスタンプを付けることになる。また、政府からの応答にも付与される見込みである。受付と応答は、電子的に行われるようになるが、内部処理は当面紙ベースのままかもしれない。これは内部処理の電子化に費用と時間がかかるためである。

(3) ハンガリーにおけるタイムスタンプ業者の動向

ハンガリーでは、今まで一部の税務処理以外、電子化を義務付けられていなかったため、企業は電子署名にもタイムスタンプにも興味がなかった。他の分野で義務付けられると、電子署名とタイムスタンプが利用されるようになると期待されている。

電子署名とタイムスタンプは、同時に使用されている。タイムスタンプのサービスだけの利用者はいない。従ってタイムスタンプサービス事業者は、CA も兼ねているのが現状である。ただし、国税だけは、タイムスタンプだけを利用している。これは税金の申告を出す時に申告日付が重要なためタイムスタンプを付けた証明書をもらう。ハンガリーの法律では、なお、申告書類は個人でも 5 年間の保存義務がある。しかしながら、ほとんどは、電子署名とタイムスタンプは同時に利用されている。

この状況が続けば電子書類が増え、電子署名とタイムスタンプサービス事業者も増えることが予想される。また、書類の保存方法が法律で明確に規定されているので、電子文書の増加とともに、保存システムの整備も必要になる。現在のところ電子書類に関して、保存・電子署名・タイムスタンプの全てを同じ企業が行っている。将来的には、その 3 つのサービスを個別に提供する事業者が現れる可能性もある。

(4) EU とのかかわり

ハンガリーは、2004 年に EU に加盟し、EU 内企業に対する自由な取引が可能となった。今後のハンガリー企業の電子署名・タイムスタンプ事業の国外への拡大が期待される。

ハンガリーの基準は、EU の基準に準拠して作成されているので、電子署名もタイムスタンプも EU 諸国内で使用可能である。しかし、ハンガリー国内と他国では、その基準に微妙な差異があるのが現状である。従って、例えばドイツへの事業拡大を狙うなら、ドイツの法律にも対応するシステムが求められる(ドイツの基準は厳しい)。

ハンガリーでは、人件費が安く、それだけ大きくコストを押さえられるメリットがある。特にインフォマティクス社は、電子署名やタイムスタンプのサービスをネット経由で100%行っていることもあり、国境のないインターネットでの事業拡大が期待されている。すでにドイツ銀行などへ食い込み始めているとのことであった。

● 質疑応答(一部、前記と重複)

Q： EU 各国は個々の法律に基づくのにハンガリーの企業のサービスが利用可能か？

A： 各国の法律は、EU 指令に従っているので、理論的には他国での利用が認められなければならない。ただし、現実にはその例がない。

Q： EU 指令には強制力は無いはずではないか？

A： 各国の法律整備が、2001 年までに義務付けられている。EU 指令は、最小限の基準であり、ドイツの基準はもっと厳しい。ドイツでサービスを提供するためには、ドイツの法律に従う必要がある。逆に、ドイツ企業は自動的にハンガリーでサービス可能である。サービス料の安さで勝負となる。

Q： なぜ安いのか？

A： ハード／ソフトは同じだが、人件費が安い(生活水準の違い)。例えば、当社は設立以来 5 年間の累積で約 200 万ユーロ（約 2.8 億円）かかったが、その 75%が人件費である。

Q： サービス料金は幾らか？

A： 利用数によって異なる。1 万～10 万利用／月で約 2 フォリント(約 1 円)。月に 10～100 程度の利用ではもっと高くなる。
ハンガリー政府は政府だけのタイムスタンプを作ることを考えている。長期間の利用ならその方が安くなりと判断している。これに 4 社は強く反対している。

Q： 電子署名のサービス料金は？

A： パッケージ販売で、2 万～5 万フォリント／年。EU の電子署名は、Advanced と Qualified の 2 ランクあり、これは Advanced の料金。国によっては Qualified しか認めないところもある。ドイツでは、我々の提供している Advanced が使えないかもしれない。

Q： ドイツ銀行で電子署名・タイムスタンプを採用していますか？

A： 現状は、採用していない。銀行にとって利益が一番であり、 電子署名・タイムスタンプを使用するような技術は素晴らしいが、経済的なメリットがないと判断しているようだ。複数の銀行を利用する顧客向けにビリングの会社が作られたが、銀行がそれを使わなくなった。

Q： タイムスタンプは今後どのような分野に使われると考えているか？

A： 将来も電子署名と同じ分野でタイムスタンプは使われる。
最も多い分野は、国との市民の間の取引、次いで電子化インボイス(請求書) の 2 つが考えられる。取引のインボイスは、業務の流れが明確なこと、紙の請求書ではその費用の大半が郵便代である。電子化すると郵送料の半額以下になりメリットがある。

Q： 印紙税のような制度はあるか？

A： 金額にかかわりなく無税である。(すなわち、印紙税削減のようなインセンティブがない)

Q： EU のインボイス指令の目的は何か？

A： インボイスを統一するためである。その結果として関税はなくなるが、付加価値税を支払わなければならない。

Q： インボイスの電子化のメリットは何か？

A： 費用が半減する、時間が短縮される。

Q： タイムスタンプはビジネスになるか？

A： まだ、採算がとれていないが近い将来は儲かると考えている。

● 考察・所感

INFORMATIKA Ltd.社の話を通じて、ハンガリー政府の電子書類への姿勢が見えてくる。日本の e-文書法との違いは明らかにならなかったが、国全体の規模自体が小さいことから、e-政府への動きは本講演だけ聞いていると順調に進んでいるようである。

しかし、一方で一般への促進には、苦心している様子が透けて見える。電子署名・タイムスタンプ業者は、これから増える可能性があるとの話だが、そもそもの現在の主要 4 社が政府主導の動きのなかで認定された印象が強く、電子署名やタイムスタンプの分野で国内の競争や流通が激しくなるのにはもう少し時間がかかりそうである。

ただ競争相手を国内に限定せず市場を EU 全体をとし、人件費の安さから国際的な競

争力を得ようとするINFOMATIKA社の姿勢は、今後のEU内での旧社会主義国家における企業の、インターネットを経由した電子文書・タイムスタンプの分野での活躍を秘めたもので、大変興味深いものである。

いずこも同じであるが、ハンガリーも電子署名とタイムスタンプの活用は官主導で進められている。民間だけの取引で利用されている例は少ないようである。

官主導と言っても二つの動きがある。一つは、規制する方向で国との取引の電子化が義務付けられて、電子署名とタイムスタンプの利用が促されるという動きである。もう一つは、規制を緩める方向で、電子的手段による取引に法的な根拠を与えることにより、利用が促進されるという動きである。ハンガリーでは前者による動機付けが大きいと思われる。

東欧中欧諸国の例に漏れず、ハンガリーも比較的に小国であるが、小さいが故にEU指令の意味が相対的に大きい。すなわち、EU指令に準拠することで、電子化に関する法制度を独自で一から作る必要がなく、また、相互認証が容易になって、EU内諸国を市場としてみることを可能としている。

小国であることをうまく活かしているようである。

５．６　DNS HUNGARY LTD.(ハンガリー)

Gabor Hirsch 氏

会議室風景

● 訪問日時：2005 年 11 月 30 日（水）　14:00～16:00.

● 場所：ホテル Aquincum 会議室

● 対応者：Gabor Hirsch 氏（IT Security Sales Manager）

● 報告者：石垣　陽　　セコム株式会社　IS 研究所　研究員
　　倉田　道夫　財団法人デジタルコンテンツ協会　企画・推進本部
　　流通環境整備部　研究主幹

● ヒアリング内容

(1)　DNS 社について

ヒアリングに協力いただいた DNS ハンガリー社は、ドイツに本社をもつディストリビュータである。ハンガリー以外にも、東欧を中心に 16 カ国（ハンガリー、チェコ、スロバキア、ポーランド、アルメニア、スロベニアなど）に支社を持っており、Checkpoint、NOKIA、Mcafee の IPS、nCipher など、様々なプロダクトを扱う。

DNS 社はここ数年、PKI、電子署名及びタイムスタンプ関係のプロジェクトに積極的に参加しており、最近では長期保管のシステムをスロベニア向けに開発した。

ハンガリーでは、EU 指令に基づいて 27 の政府サービス電子化に向けた取り組みが行われており、DNS 社では、これらサービスの基準づくりに積極的に参加しているという。政府の電子サービスの１つに、電子行政を実現するための「e-Gate」と呼ばれるサイトが挙げられる。これはハンガリー国民及びハンガリー企業向けの行政ポータルサイトであり、

既に金融庁が企業年金の電子サービスを提供している。また、会社設立の登記についても、電子化が検討されている。

(2) ハンガリーの PKI 事情

Gabor 氏によれば、現在ハンガリーでは 4 つのクオリファイド認証局が存在するという。クオリファイド認証局には、タイムスタンプサービスを運用することが義務づけられているため、4 社全てがタイムスタンプサービスを提供している。認証局及びタイムスタンプ局は、EU 指令及び国内法に準拠しており、厳しい認定審査基準を満たしている。

① NetLock（http://www.netlock.hu/USEREN/index.html）
ハンガリー初のクオリファイド認証局で、1996 年に設立された。CA と TSA を自社開発し、運用している。

② Microsec
RSA の Keon Certificate Authority 及び、nCipher の HSM を利用している。認証局の一部は、自社開発している。

③ Magyar Telekom（マジャルテレコム、http:// www.magyartelekom.hu/）
ドイツテレコムの子会社で、ドイツテレコムが開発した CA や、nCipher の HSM を採用している。

④ Mav Informatika（http://www.mavinformatika.hu/）

(3) 電子インボイスサービスの紹介

ハンガリーでは、2004 年 5 月からインボイス（請求書）の電子化が認められた。この法律では、インボイスへの電子署名は義務づけられているものの、タイムスタンプの付与は義務化されていない。しかし、インボイスに関連する他の法律によって、以下の要件が加えられる。

- タイムスタンプの付与
- 5 年間の保存義務
- 政府審査を受けたサービスプロバイダーにおけるアーカイブ（必須ではない）

こうした法制度の下で、マジャルテレコム社は 2006 年から、電子インボイスのサービスを開始し、自らがそのユーザーとなっている。これによってマジャルテレコムの顧客は、希望すれば電子インボイスサービスを利用可能となる。

質疑応答

Q： マジャルテレコム社以外にも、電子インボイスを利用する動きはあるのか？

A： 今のところ、電子インボイスのユーザーはマジャルテレコム社しかない。マジャルテレコム社の顧客は、希望すればこの電子インボイスを利用できるようになるが、いくつかの問題を乗り越える必要がある。まず電子インボイスを利用するためには、クオリファイド証明書の購入や、専用の IC カード、ソフト、規定されたハードウェアの利用といった投資が必要となる。インボイスだけでなく、業務プロセス全体を電子化することによる長期的なコストメリットを見いだすことで、初めて電子インボイスの利用が促進される。また現在の法制度では、ハッシュだけでなく、原本（電子インボイスの場合は、インボイスのコンテンツ）も TSA 側に送らなくてはならないことになっている。これについて、技術的な不効率性や、情報漏洩の懸念を抱く声が多い。

Q： クオリファイドの証明書は普及しているのか？

A： アドバンスドの方が、クオリファイドと比べて良く売れている。クオリファイドは利用目的が限定される上に高価なため、普及はこれからと考えている。なおクオリファイド認証局は、厳しい認定審査基準を満たす必要があるが、この基準についても改善の余地がある。例えば、CC（Common Criteria）は認定基準として認められているが、FIPS は認知されていない。このため、FIPS 認定を受けた製品をハンガリーで利用する場合、追加の審査が必要となることがある。

Q： EU 指令や日本の e 文書法で示されているような「電子化」は、ハンガリーはどのように取り扱われているか？

A： 現在のところ、国内法では特に規定が無く、電子化を行うことは想定されていない。将来、認められるようになるだろう。

Q： 2003 年に EU 指令で電子調達が勧告されたが、ハンガリーでは何か動きがあるか。

A： 電子調達については、インボイスや企業年金の電子化と比べると消極的と言わざるを得ない。

Q： タイムソースはどのような構成になっているか？

A： 現在、最低 3 カ所から得ることになっている。ドイツ（バーンシュタイン）にある PTB からの配信、原子時計、GPS などが挙げられる。

Q：　アーカイブサービスを行っている会社はあるのか？

A：　今のところ、アーカイビングを行っている会社は無い。

Q：　電子インボイス利用のためにアーカイビングが推奨されているようだが、これはどういった理由によるものか？

A：　認証局 4 社の強いロビー活動による。これはあまり健全な姿ではなく、改善を求める議論もある。

【写真 5-6-1】ホテル Aquincum 会議室前にて

５．７　Viasec、Slovenska technicka univerzita、Min. of Defence National Measurement Institution（スロバキア）

Ing. Mach Martin 氏

doc. Ing. Ladislav Hudec,CSc.氏
Capt. Rene' Stevonka 氏
Capt. Rudolf UrSanovsk'氏

Mr. Pavol Dorsic 氏

- 訪問日時：2005 年 12 月 1 日（木）　14:00～16:00

- 場所：Viasec オフィス

- 対応者：・Viasec
  Ing. Mach Martin 氏（manazer IT）
  Ing. Batek Ľubos 氏（riaditel）
  ・Slovenska technicka univerzita（スロバキア技術大学）
  doc. Ing. Ladislav Hudec,CSc. 氏
  （Katedra informatiky a vypoctovej techniky）
  ・Min. of Defence（スロバキア国防省）
  Capt. Rene' Stevonka 氏
  Capt. Rudolf UrSanovsk' 氏
  ・National Measurement Institution（スロバキア国立測量研究所）
  Mr. Pavol Dorsic 氏　(Centre of Length and Time)

- 報告者：三谷　慶一郎（株式会社 NTT データ経営研究所
  情報戦略コンサルティング本部長　エグゼクティブコンサルタント）
  清松　哲郎　（株式会社東大総研　理事）

● ヒアリング内容

（1）Viasec＆Slovenska technicka univerzita

今回の出席者は、みんな Viasec のパートナーである。国立測量研究所からは、時刻の配信についての話をする。スロバキア技術大学の教授は、タイムスタンプの研究家である。防衛庁は、タイムスタンプのユーザーである。

まず、タイムスタンプ、認証、電子署名法について話をしていきたい。

スロバキアの電子署名法は、2002 年にできた。スロバキアは EC に加盟したので、署名法を早急に策定しなければならなかった。この法律には、証明書、タイムスタンプをどう使うかが書いてある。

電子署名法には、大きく二つの内容が書かれている。ひとつは、タイムスタンプをビジネスにおいてどのように使うか、もうひとつはタイムスタンプを行政機関とのコミュニケーションにおいてどのように使うかである。

EU 指令においては、3 つの種類の電子署名がある。これらは信頼性が異なるものである。低いレベルのものは、鍵がなくても大丈夫である。最上位のものは、スマートカードに鍵を記録しておくことが必須となる。

電子認証局についても署名法において整理されている。認証局には認定制度があり、そのためには厳しい監査も必須であり、安全記録のコントロールも必要である。Viasec は、認証局を運営しており、信頼性の高い証明書を発行している。

スロバキアの電子署名法では、証明書のセキュリティレベルは定義しておらずクライアントとの相談で決定する。但し、これはビジネスの場合（民間分野の場合）のみで、行政機関とは一番信頼性の高い証明書が必要となる。

行政機関への電子署名の導入は、コストと時間がかかる。しかし信頼性の高いコミュニケーションが成立するので、タイムスタンプが使われた書類は、問題なく証拠となると考えている。行政機関とのコミュニケーションには、HSM が使われており、EAL のレベル 4、FIPS も必要とされている。

スロバキアでは、行政機関に対して電子認証とタイムスタンプを使うプロジェクトが現在いくつか推進されつつある。

ひとつは、税務署とのコミュニケーションである。これは、大企業が主に利用するプロジェクトである。現在はあまりまだ普及段階にはないが、今度の 3 月には年度末なのでトラフィックは増えてくると考えている。

税関とのコミュニケーションにおいても電子化が推進されている。これは、企業のコスト削減にかなり結びついている。約 100 億コロナ（約 377 億円くらいの削減額になるのではないだろうか。スロバキアへの輸入時の関税手続きは今まで 2 日間必要であったが、インターネットを利用することによってかなり短縮できるようになった。

デジタルインボイスも今、3 社程度で準備中である。来年くらいから実際に開始されるのではないかと思う。例えば当社でも現在、ISP を対象としたものを考えている。ISP

に対して加入者は、月に 400 コロナ（1500 円）位払っているが、そのうち 30 コロナ（133 円）はインボイスにかかっている。ここにデジタルインボイスを適用したい。

その他、実現が近いものとしては、健康保険、社会保険の電子化がある。全ての大企業では毎月従業員の情報を送っており、これは 4 万社くらいになる。この部分の電子化である。

政府は、インターネットによるコミュニケーションを重要視しており、「プロジェクト・ミネルバ」というものが立ち上がっている。プロジェクト･ミネルバは 27 項目から構成されている。例えば、個人からの申請とか報告などの電子化が構想されている。

また、行政機関間のコミュニケーションについても構想されている。今はあまりこれらのコミュニケーションは取られていないのではないかと考えられており、インターネットが有効ではないかといわれている。この部分にも電子署名を使う予定である。

重要な項目としては、個人が持っている ID カードにチップを埋め込み証明書を格納できるようにする取組みがある。

インターネットによる選挙も構想されている。

現段階の電子署名、タイムスタンプについては、問題もいくつかある。

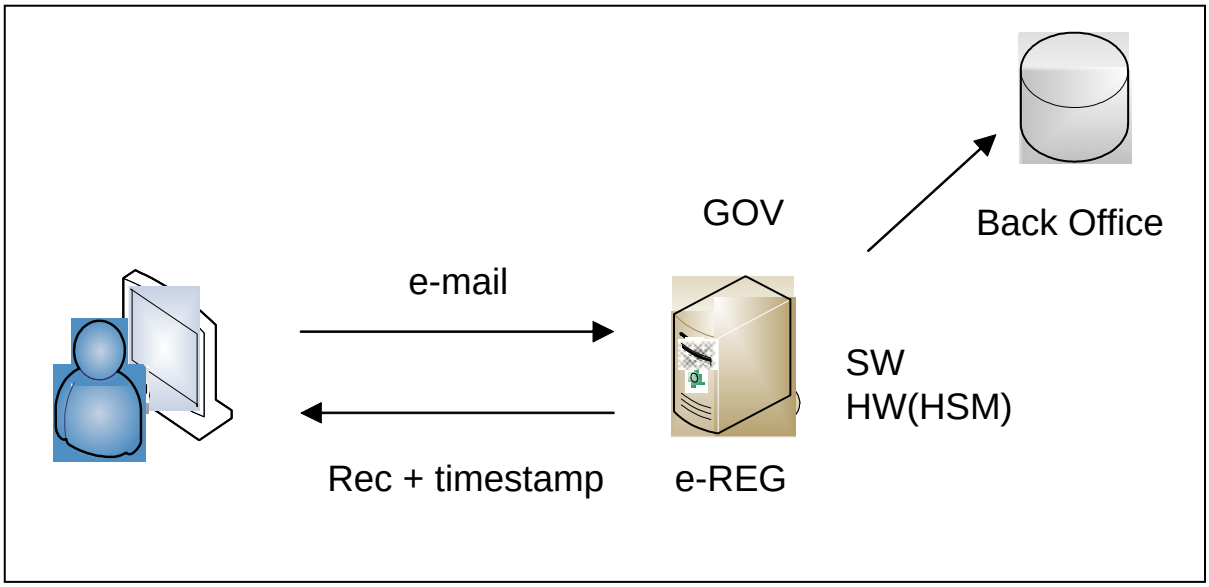
ひとつには、正確な時刻のソースを得るためのインフラがまだできていないこと。また、現在の電子署名法が、「個人」のみ対象としているのでチューニングが必要となっている。更に暗号化・セキュリティ・プログラマー等の資格を持つ人材が少ないことも問題である。

スロバキアの電子署名法は、EU 指令とは相違している部分がある。EU 指令は広く曖昧。これに対して、スロバキアではずっと厳しい条件になっている。これは、国家がその信頼性に対する責任を取らなければならないからである。

スロバキアの電子署名法は、最初に策定するときはどちらかというと「厳しく」する方向で考えた。例えばチェコはそんなに厳しくない。現行法制度に問題点はあると思うが、ポジティブに捕らえている。

スロバキアの電子署名法は、当初、厳しくした策定したわけだが、今後はある程度「弱く」していくことを考えている。策定後 3 年間の実績・経験を踏まえ、これを反映させることを考えている。

現行の電子署名法のひとつの問題は、電子署名法の対象が個人か CA だけであり、機械（サーバー）は対象にならないことだ。例えば、行政機関で推進されている「窓口」である e レジストリではタイムスタンプが必要となっているが、これは現行法制度ではカバーができない。これについては、国家安全保障局が「例外のケース」と現在は整理している。行政サービスに対しては、e レジストリが必須となっており、ここではタイムスタンプが必須となっている。



【図 5-7-1】e レジストリ・イメージ図

現在、スロバキア内の認定認証局は、Viasec、PSCS、DTCA という 3 社である。ちなみに認定外の認証局は 5 社ある。現在は認定外の CAEVPU も認定を取ろうとしている。

認定認証局 3 社のうち 2 社は、タイムスタンプサービスを提供している。タイムスタンプサービスと合わせ、フルサービスを提供することは事業から見て有益であるといえる。

（2）National Measurement Institution

National Measurement Institution は、現在スロバキアにおける唯一の時刻発信源となっている機関である。HP5071 の原子時計を使っており、GPS を使って UTC とコミュニケーションを取っている。

ちなみに本研究所は国際会議メンバーである。ご案内の通り、日本もメンバーの一員である。

時刻については「測量法」という法律で基準などが決まっている。

時刻の客観性は、いくつかの観点から保証されている。本研究所が国家研究所であること。時刻が Web ページに公開されていること。100 ナノ秒の高精度を維持していることなどがその理由である。

前出の「正確な時刻のインフラが未整備」というのは、現在、時刻源から TSA へ時刻が連動できていないことを意味している。そのため Viasec の TSA は現在、米国 NIST に接続している。研究所では、まだ TSA と連動するためのハードウェアが準備されていないが、これは来年中に準備できる予定、あくまで財務省の予算次第ではある。インフラが準備できれば TSA には無料で提供する予定である。

（3）Min. of Defence

国防省とその関係管理部署との効果的なコミュニケーションのために、インターネットを利用している。郵便物では 3 日もかかってしまう。この領域に、電子署名とタイムスタンプを使っている。

国防省と他省庁とのコミュニケーションについても適用を考えている。これらのコミュニケーションには、XML ドキュメントを導入することを予定している。

電子的コミュニケーションにおいて電子署名、タイムスタンプを使っているのは、国税庁と国防省が中心である。

国防省がこれらの技術を導入しているのは、重要な情報を扱っていることもあるが、NATO 加盟国だから、というのもある。NATO では、加盟国どうしで様々な共通規約を作り始めている。タイムスタンプや電子署名ももちろん入るはずである。

電子的なコミュニケーションの対象となっているドキュメントは、業務に使っている書類の全てである。機密性が高いドキュメントについては、さらに秘匿性の高い措置を行うこともある。

タイムスタンプを利用するのは、それがいつ作られた書類なのかをわかるようにするためである。締め切りなどがある場合には有効である。タイムスタンプを利用するのは電子署名だけでは不十分なためである。

電子文書を保管する場合には、時間の経過と共に電子署名の力は弱くなっていく。（筆者注：暗号の危殆化の意味か？）これはなかなか解決できない問題である。電子文書の長期保存においては、タイムスタンプのリスタンプを行うことも考えている。

● 質疑応答

Q： 電子署名法立法時に、まず高いハードルで設定したのはなぜか？あまり高すぎると技術が普及しないように思えるが？

A： 潜在的にある危険から国家として回避するため。電子署名は重要な技術であり、低いハードルにすると、悪い方法で不正に使われてしまう可能性が出てくる。また、私見であるが、やはり国家安全保障局が作ったということ自体が理由でもあるのではないか。

Q： タイムスタンプを単独で利用することは考えていないのか？日本では知財のような分野ではそのようなニーズがあるといわれているのですが？

A： タイムスタンプ単体では考えていない。あくまで電子署名と結びついていると考えている。

Q： 電子署名法のレベルの話が出たが、どのような国が高いハードルを課しているのか？

A： EU の中でどの国が厳しいのかはわからないが、例えばハンガリーはスロバキアの電子署名法を参考にしているという話は聞いたことがある。また関連した話としては、EU で「ブリッジ・プロジェクト」というものが推進されている。これは、FESA が担当しているもので認証局の横断的橋渡しについて検討するものである。

Q： 防衛庁での電子的コミュニケーションにおいて WORD を使っているのか？

A： WORD は使っていけないことになっている。マクロが見えなくなるので。使っていいものは、RTF、PDF、XML、TXT、MIME である。

● 考察・所感

SI ベンダー、NTA、行政機関、研究者を一同に集め、関係者も含め 20 名近くの方々を対象としたかなり中身の濃いディスカッションになった。限られた時間ではあったが、スロバキアにおけるタイムビジネスの概況をつかむことができたと考えている。

日本では、あまり情報が得られず、一般的には IT に関しては先進国とは見なされることが少ないスロバキアではあるが、思った以上にタイムビジネスが現実のものになっているようである。

注目したいのは、タイムビジネスを推進していく中心が電子政府分野であることである。行政機関自体が、民間に先んじて、自らの電子的コミュニケーションにおいてタイムスタンプを率先して利用しようとしている。また、先導的な役割を担っているのが、重要な電子文書を扱っている国税庁と国防省であることも興味深い。

もう一点、タイムスタンプは単独で使うのではなく、電子署名とセットで使うものだという考え方が浸透していることもわかった。これは、日本と EU との電子署名法のカバー範囲の違いから来るものであるのは間違いないだろう。長期保存を前提とした電子的コミュニケーションを実現する場合には、電子署名とタイムスタンプによってその原本性を確保するという考え方には全く異論はない。

【写真 5-7-1】会議風景

【写真 5-7-2】Viasec 会議室にて

Viasec、Slovenska technicka univerzita、Min. of Defence

National Measurement Institution メンバー，TBF メンバー

５．８　SETCCE　（スロベニア）

MAP（スロベニア）


mag. Tadej Puki 氏

● 訪問日時：2005 年 12 月 2 日（金）　14:00～16:30

● 場所：Viasec 社 会議室（スロバキア）

● 対応者：mag. Tadej Puki 氏 (Maketing Manager)

● 報告者：林　誠一郎（株式会社ＮＴＴデータ　ビジネス開発事業本部
セキュリティビジネスユニット
エグゼクティブ・セキュリティマネージャ）
井山　泰裕（株式会社ＮＴＴデータ　ビジネスソリューション事業本部
セキュリティサービスユニット　セキュリティビジネス担当）

● スロベニア共和国概要

スロベニア共和国は、1991 年に旧ユーゴスラビアから独立した人口 200 万人の小国である。旧ユーゴにおける先進工業地域であったため、独立後は市場経済化、西欧諸国との関係強化を進め、現在は中・東欧諸国の中では最高水準の GDP を誇っている。2004 年には EU 加盟を果たしている。

● ヒアリング内容

(1) SETCCE 社について

SETCCE（Security Technology Competence Center）社は、スロベニアで権威の高いヨセフ・ステファン研究所から派生した企業である。社員数 15 名の若い会社である。主に、スロベニア国内においてシステム構築や、PKI 関連の開発やサービス提供を行なっている。特に、PKI に関しては 10 年以上の開発実績がある。近年では、EU の通信セキュリティや個人情報保護のリサーチプロジェクトへの協力や、政府の電子署名導入プロジェクトに関与している。

(2) スロベニアにおける電子署名の現状

スロベニアの電子署名法は、EU 指令に基づいて 2000 年に施行された。法律の制定は、電子化の推進によって紙文書を減らすことを第一の目的としている。現在、スロベニアの人口は 200 万人であるが、そのうち 10%にあたる 20 万人が電子証明書を保有している。この法律は認証局の認定制度も定めており、現在、認定を受けたクオリファイド認証局は国内に 4 つ存在している。内訳は、「銀行」「郵便局」「政府機関」「民間企業」である。

- 「銀行」
  国内の銀行業務のシェア 40%を握る大手行である。オンラインバンキングサービスを提供しており、その利用にクオリファイド証明書を使用する仕組みを導入している。電子証明書の格納媒体には、USB セキュリティートークンを採用している。
- 「政府機関」
  全国民の所有する ID カードを、すべて IC カードへの切り替えるプロジェクトを進めている。IC カードには電子証明書が入っており、国民は無料で取得できる。利用用途としては、Tax の申請などが実用化されている。

これら 4 つの認証局の Root 証明書は、スロベニア国家安全局（NSA）によって発行されている。NSA の自己署名証明書は、有効期限を 2014 年までと定めている。（有効期限を 2014 年に設定した明確な根拠は無いようである。）そのため、各認証局はエンドユーザー向けに、最大で 2014 年まで有効な電子証明書を発行することもできるが、ビジネス面から有効期間 1 年の証明書を発行している。

(3) スロベニアにおけるタイムスタンプの現状

タイムスタンプサービスは郵便局と政府機関が提供している。1 スタンプあたり 1～4 セントユーロで販売しており、銀行がログにタイムスタンプを付与するためや、e-keeper の利用者が購入している。タイムスタンプサーバに用いている電子証明書は、認証局と同

じく NSA が発行している。そのため、タイムスタンプの有効期限も 2014 年までとなっている。

(4) SETCCE の製品について

SETCCEは、

- EU指令及び各国法律に批准
- グローバルスタンダード準拠
- 高いレベルのセキュリティ

を柱に現在のビジネスプラクティスにPKIに基づくセキュアな電子化をもたらす製品開発を行っている。現在は、他の製品開発を行っておらず、既成製品のアップグレードに力を入れている。SETCCEは、PKIに関する4つ製品を展開している。

① proXSign

電子署名とタイムスタンプを使用するためのライブラリである。既存システムに組み込むことができ、ERP、電子インボイス、 製薬システム、e-Banking やワークフローエンジンなどへの利用を想定している。使用するタイムスタンプは、RFC3161 に基づいて、エントラストの電子証明書を用いたもので実績がある。

② WebSign

XML 電子フォームを回覧するためのワークフローシステムである。proXSing と連携することで、一つの書類を回覧し、複数の人が電子署名するという利用が可能である。電子稟議、電子インボイスや電子契約などが想定される。実際の利用例として、インターネットサービスプロバイダ（ISP）への申し込みや、学生人材派遣の電子契約がある。

- 「ISP の申し込み」

  顧客が Web サイトからオンラインで申し込み、契約を行う。Web ブラウザと ActivX を用いて、申込書に電子署名を付与している。

- 「学生人材派遣の電子契約」

  企業の学生アルバイト雇用において、企業は学生人材派遣会社と契約を結ぶ。この雇用契約を、電子署名を用いた電子契約で実施している。スロバキアの法律では電子契約に電子署名は必須ではないが、利用者の自主判断で電子署名は行なっている。

③　eBiller

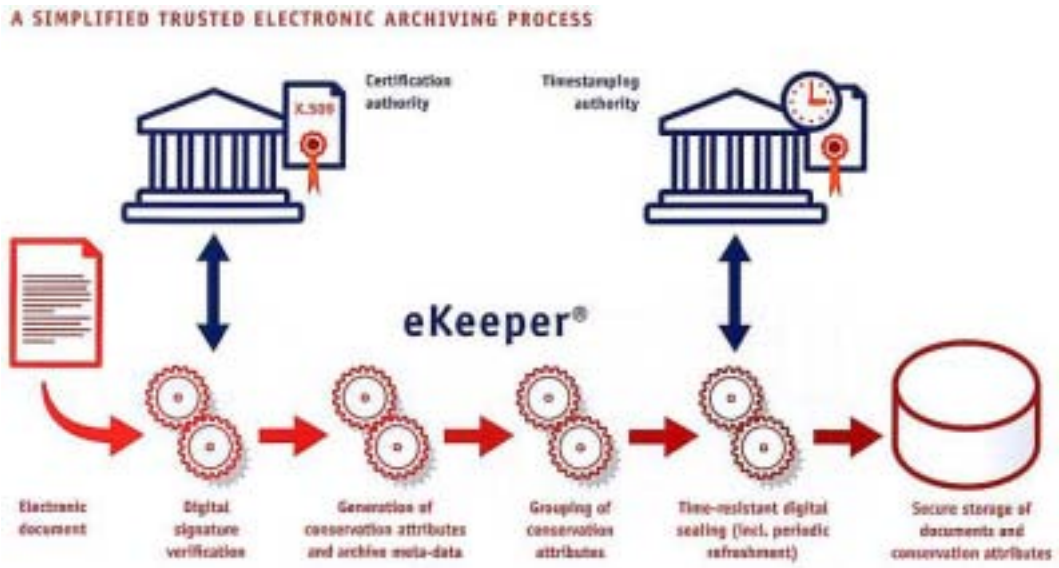
大企業を対象とした電子インボイスや、銀行のステートメントを収集、発行、管理するシステムである。社内の ERP から自動的に電子インボイスを作成することができ、電子署名とタイムスタンプを自動的に付与して E メールで送付する機能を有している。

【図 5-8-1】　eBiller プロセス

④　eKeeper

eKeeper は電子文書（電子署名の有無は問わない）を長期的に保管するシステムであるが、電子公証を行なう機能も有している。電子文書が改ざんされないように保管することはもちろんであるが、Conservation Attributes（C.A）と呼ばれる管理情報に電子署名とタイムスタンプを付与することで、電子文書の改ざんを検知でき、法的にも有効であることを証明できる。また、タイムスタンプのコストを削減するため、複数の電子文書をまとめてタイムスタンプを付与する機能もある。また、それらの文書の原本性を個別に検証したり、保管年限の過ぎた文書を保管対象からはずしたりしていく機能も有している。電子署名の有効期限切れについては、①失効の 1 カ月前までに再署名する、②公証人に公証してもらう、③予めタイムスタンプを付与しておく、のいずれかを実施することが決められている。しかしながら、スロベニアの法律ではタイムスタンプの付与は義務化されていない。もしもタイムスタンプを付与した場合の有効期限切れについては、失効の 1 カ月前に再スタンプをする機能を実装している。

eKeeper は国防省で使われており、国防省はすべての書類をスキャンして電子保管している。民間では“Simobil Vodafone 社”が電子インボイスを 10 年間保管するために利用している。他にも国内最大手の ISP もこのシステムを導入している。



【図 5-8-2】　A SIMPLEFIED TRUSTED ELECTRONIC SRCHIVING PROCESS

● 考察・所感

スロベニアでは、国民の 10 人に 1 人が電子証明書を保有しているという普及率には驚かされる。タイムスタンプの利用は義務化されていないこともあり、まだ一部に留まっているようであるが、電子署名がオンラインバンキングなどで利用されており、電子署名の普及とともにタイムスタンプの利用もスロベニア国内で広がりを見せる可能性があり大変興味深い。今回の SETCCE 社との会談は、SETCCE 社の製品説明の色が濃くなってしまい、スロベニアの電子署名やタイムスタンプの制度に関して十分なヒアリングができないまま時間切れとなってしまったのは、いささか残念ではあった。しかし、スロベニアは今後注目していくに値する国の 1 つではないだろうか。

【写真 5-8-1】SETCCE

おわりに

タイムビジネス推進協議会の今回の海外調査は、前回に引続き、欧州をターゲットとし、「タイムスタンプの利活用」をメインテーマに、イギリス・ハンガリー・スロバキアを訪問した。

訪問先の選定・調整において全面的にご協力いただいた nCipher 社の皆様、今回の調査全体の企画を受け持っていただいた日本ツーリスト開発株式会社の皆様にまずは深く御礼申し上げたい。

今回の海外調査ではタイムビジネスに関して新たにいくつかのメッセージが得られたと考えている。詳細は、本文中に譲るとして、ここではその概要をいくつか述べていきたい。

まずご報告しなければならないのは、欧州特に東欧においても、電子データ流通・保存の場面において利用者側はタイムスタンプを十分意識し、確実にそれを利用していたことである。

イギリスはともあれ、今回回ったハンガリーやスロバキアといった東欧諸国は、「IT」というテーマでは、あまり先進的だとは（少なくとも私たちの周囲においては）みなされていなかった。そのような国々において、タイムスタンプをサービスしている電子認証局が各国複数社既に立ち上がっており、普及はともあれ、具体的なアプリケーションにおいてタイムスタンプが利用されていることは正直驚きであった。

今回のテーマである「利活用」という観点では、電子政府分野の話題が多かった。

ハンガリーの国税庁における電子申告、スロバキアの電子政府推進プログラム「プロジェクト・ミネルバ」における、関税手続きの電子化、防衛庁等中央省庁間におけるデータ交換等において、タイムスタンプの活用が現実のものになっていた。

電子契約や e-文書法等、民間分野における電子文書流通・保存においてタイムスタンプの活用が先行している日本と比較して、今回訪問した欧州諸国では行政分野において重要文書へのタイムスタンプ適用を行うことによって、行政自体がこの領域を先導しようとする意気込みが感じられた。タイムスタンプサービスを提供する電子認証局のいくつかが半官半民的なプレイヤーによって運営されていることもその裏づけのように思える。

今回の訪問先が東欧中心であったことも行政主導色が強かった理由のひとつなのかもしれないが、電子政府先進国として自他共に認められており、電子認証基盤の整備が進んでいる日本の行政分野において、あまりタイムスタンプへの言及がないのはやはりアンバランスに思えてならない。今後は推進協議会としても当該分野への働きかけを強化していかなければならないと考えている。

もうひとつ、利活用の対象として、いわゆる「デジタルフォレンジック」分野に関する話題も出てきた。米国で 2002 年に制定された「Sarbanes‐Oxley act」のような、企業における企業会計や財務報告の透明性・正確性を高めるために、健全な内部統制を義務化するような流れは、既に日本でも検討されつつある。このトレンドは欧州でもやはり同様のようで、類似のルールがいくつか作られつつあるようである。

このような流れを踏まえ、情報システムが正常に稼動した証拠となりうるデータ、例えばログなどに対してその完全性を確保するためにタイムスタンプを適用するというニーズは顕在化されつつあるように見受けられる。協議会でもこの分野の可能性について話をし始めていたところではあったが、さらに検討を深める必要がある。

タイムスタンプの位置付けについても日本との違いを感じさせられた点があった。

欧州においては、タイムスタンプは PKI 等の電子署名との組み合わせで語られることがほとんどのようである。これは欧州において、電子署名とタイムスタンプが同じ電子署名法の枠組みの中で整理されていることが大きな理由である。

一方、日本の電子署名法ではタイムスタンプについての言及がなく、タイムスタンプは比較的単独で語られる機会が多い。日欧の違いは法律の立法目的・背景の違いのためだと想像できるが、いずれにせよ、欧州と同様に、「電子文書を流通させ、保存する際には電子署名とそれを補完するためのタイムスタンプが必要不可欠である」というメッセージをわが国においても一般化させることは急務である。

電子署名法といえば、スロバキアで興味深い話をお聞きした。スロバキアでは、高いハードルを課していた電子署名法を、低くする方向で見直しを行う予定があるとのことだった。ルールの厳格性とマーケットへの普及・啓発との関係については、当協議会でもよく議論になるテーマなのだが、いったん立法したものを絶対視せず、その後の状況や市場環境を踏まえて早めにチューニングしなおすことはなかなかできることではない。先端で技術進歩の早い領域におけるルール作りにおいては、このようなフレキシビリティの確保は重要な要素ではないだろうか。

最後に、イギリスで話題になった「電子文書の長期保存」について触れておきたい。

現在氾濫している元々が電子データ（born-digital）である電子文書を、10 年、20 年あるいは 100 年以上というスパンで長期的に保存し続けるというニーズは間違いなく今後増えてくる。今回意見交換した大英図書館は文化的観点からその必要性を認識しており、独自に長期保存検討のためにプロジェクトを立ち上げていた。

このようなニーズに対しては、電子文書についてその証拠力を向上させるための包括的な検討が必要となる。現在のタイムスタンプ技術の強化はもとより、「可視性」、「保存性」といった全く別の観点についての技術的対応策も議論の対象となるのである。

国際的にもまだ「正解」のない電子文書の長期保存というテーマについて、日本発の提案を示すことができればその意義は大きい。当推進協議会も是非本テーマについては、検討への貢献ができればと考えている。

本書は事実報告を中心に取りまとめた当面の成果である。

今後さらに得られた知見をベースに分析を深めていきたい。そして今回の調査結果についてたくさんの方々と議論を交わすことができればこれに勝る幸せはない。

平成 18 年 1 月

タイムビジネス推進協議会　企画部会長
株式会社 NTT データ経営研究所
三谷　慶一郎