

## T-Scheme 概要

このドキュメントは、tScheme に関する調査レポートです。

tScheme に関する最新の情報等については、

<http://www.tscheme.org/>

を参照して下さい。

---

# T-Scheme 概要

(株)NEC 総研

2002年2月7日 (v0.4.3)

英国の内閣府は現在、T-Scheme といわれるスキームを通して文書を公開することを義務付けている。これは、メタデータを付与したかたちでの情報公開を前提にした仕様であり、情報の信頼性や利便性を向上させることを目的としている。T-Scheme は、国内外の多用途での電子化促進のため仕様が広く公開されており、また英国政府から独立した標準化団体が設置されている。このようなことから、特に欧州を中心に、政府の開発した認証システムを民間のEコマースに応用する動きが活発になってきている。

## 1. はじめに – T-Scheme とは

T-Scheme は、政府のサポートを受けたセキュリティ対策に関する標準である。電子商取引を行なう企業と、認可を受けた「トラスト・サービス・プロバイダ (trust service providers)」の両者によって構成されるシステムで、メッセージは電子署名によって漏洩や改ざんから保護される。これは、公的な文書の公開や各種行政サービスや納税等の手続きを円滑にする目的で英国政府が導入を進めている PKI<sup>※1</sup> システムであるが、現在ではむしろ、民間企業のオンライン取引における基盤整備としての位置付けのほうに

より高い関心が集まっているようだ(図1参照)。

トラスト・サービス・プロバイダは、電子署名を行ない、配信過程での改ざんがないことを保証し、それが機密のままであることを確認するメッセージの通知を許可する。これにより、オンライン不正行為の機会は縮小される。

これは、ごく小規模な取引においてはやや大きな仕組みに見えるかもしれない。しかし、今後企業の税務申告や個人の抵当申し込みなどを通じて、このような信頼性の高い商取引環境は、電子商取引の本質的なメリットとして認識されるようになるだろう。

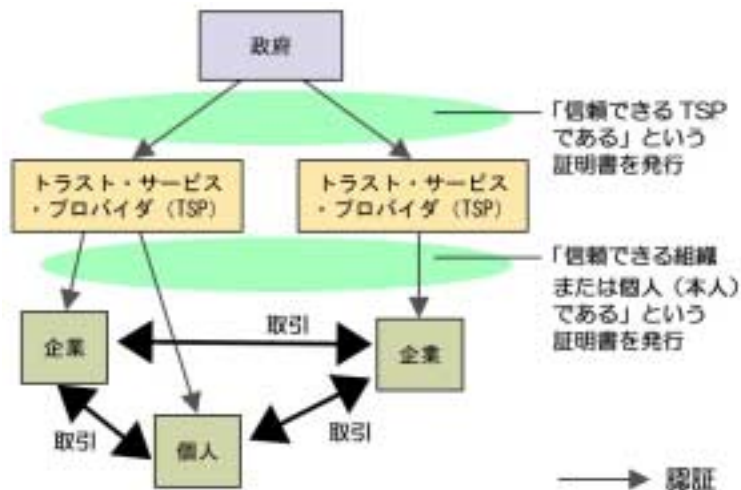


図1 信頼性の高い電子取引を実現するT-Schemeの基本的な仕組み

## 2. 各国における電子政府の取り組みと認証基盤(PKI)

迅速化を進め情報の統合的な扱いを可能にしようという取り組みは、1990年代の中ごろから、米国、英国、シンガポールを始め、各国で行なわれている。特に、認証基盤の整備(PKIの認証局の設置、デジタル

「電子政府」のコンセプトのもとに、行政の効率化や

※1 PKI … 「公開鍵基盤(Public Key Infrastructure)」: 公開鍵暗号技術と電子署名を用いることにより、コンピュータ・ネットワーク(特にインターネット)を使用した通信を安全なものにするための環境基盤。

署名等に関する仕組み作り)に関しては、ほとんどの政府機関で導入され、実用化が始まっている(認証方式としては PKI のほか、PIN 番号の利用や Shared Secret/キーワード照合といった方式が採用される場合もある)。

米国では、大統領選で財政赤字の削減と行政に対する国民の信頼回復を公約に掲げていたクリントン政権が、行政改革(Reinventing Government)の柱として電子政府化に注力。1995 年には、「2004 年までに連邦政機関の総調達のうち 95%を EDI 化する」という方針をまとめている。また、電子署名が紙の署名と同等であることを認める法案が 1999 年 11 月に上院で可決されている。英国では、1996 年のグリーンペーパーを契機に、Information Society Initiative の一部として電子政府プロジェクトに着手。その他欧州では、EU 加盟国の法律に基づき、完全で有効な共通のフレームワークの実装が進められている。欧州委員会の「電子商取引におけるヨーロッパのイニシアチブ」では、電子商取引のための主要な課題として、電子的署名の必要性が確認されているが、これは電子商取引での契約交換の署名は、グローバル市場での競争において、ヨーロッパのビジネスの必須要素になりうるという考えからである。また、シンガポールでは、1995 年より Connected Government プロジェクトを開始し、行政サービスにおけるスマートカードの活用、情報キオスクでの自動車保有更新手続きなどを実施している。

各国が行なう電子政府への取り組みの課題として現在、PKI など一部のサービスを民間に開放することや、国際的な連携の強化などが重点的に扱われている。

マイクロソフトは、電子政府フレームワーク

(Electronic Government Framework)を世界各国に提案しているが、これは XML (eXtensible Mark-up Language)、XSL (eXtensible Style-sheet Language)、SOAP(Simple Access Protocol)のようなオープンな技術を積極的に採用したもので、固有のベンダに依存しないフレームワークとして高く評価されている。

T-Scheme もまたオープンな仕様であり、政府 PKI を標準的な技術で構築することによって開発コストを削減するとともに、利便性を高めようという試みの一例と見ることもできる。

EU 加盟国では、評議会の要請にもとづき「電子的署名に共通の枠組みを提供するよう指令が出されているが、この要件に応えるために、ヨーロッパ電子的署名標準化活動(EESSI: European Electronic Signature Standardization Initiative)が発足している。英国では、国際標準に準拠しながらも、欧州各国と研究・開発や評価で緩やかに協調し、またこれら EU 加盟国と同様に「認証局に対する任意的な資格認定制度」を採用している。このようなことから、英国が、EU 加盟国を含めた国際的な連携体制を築きたい意向であることが伺える(表 1 参照)。

### 3. 英国の電子政府戦略

英国では、「電子政府は、情報化時代における公共サービスの基本戦略である」としたうえで、2005 年までに官庁業務を 100%電子的に実行できるよう、電子サービス提供の準備が行なわれている。また、2002 年までに世界最高の電子商取引環境を構築す

表 1 英国および EU で導入されている PKI

国	名称または運営母体	基盤となる技術	国際標準への準拠	概要
英	T-Scheme	PKI solutions.	○	英国では信頼性保持のため、産業ごとに信頼性の基準を定めている。T-Scheme では、トラスト・サービス・プロバイダ(恐らくは英国の政府を含む)に対して、証明書発行のための仕様を定義している。
英	CLOUD COVER	PKI	○	英国政府系機関のため、最低限の PKI 相互運用基準を定めた政府スキーム。これは英国の行政サービス部門の一部である CESG(政府のための最上位の認証局)によって運用される。
EU	EESSI (The European Electronic Signature Standardization Initiative)	PKI x. 509	△	任意で、署名生成方法や署名認証などのため、EU 全体の標準化や認可を行なう。また、公的な資格を満たす証明書を発行するトラスト・サービス・プロバイダを監督する(登録や通知は、QC ポリシー実現のため、自己宣言制)。標準に関連する仕事は、CEN および ETSI(EU 全体の標準化団体)によって行なわれる。

参考: GENERAL USAGE FOR INTERNATIONAL DIGITALLY ENSURED COMMERCE version II  
([http://www.iccwbo.org/home/guidec/guidec\\_two/GUIDECappendix.pdf](http://www.iccwbo.org/home/guidec/guidec_two/GUIDECappendix.pdf))

る計画があるが、これも電子政府の開発に高度にコミットしたものだ。

注)1999年3月に公表された「政府近代化白書(MGWP)」では、「官庁の25%が2002年までに電子配達、2005年までに50%、2008年までにすべてのサービスを電子化」とされていたが、英国首相はこの目標を前倒しし、サービスの全てを電子的に行なえる「電子政府」の開発を2005年までとした。

英国は、PKI に関する必要条件を満たす市場およびコミュニケーション・エレクトロニクス・セキュリティ・グループ(CESG)に目を向けている。これには、次のようなものがある。

- 政府省庁が広範囲な安全保証を行なう CLOUD COVER プロジェクト<sup>※2</sup>
- 相互運用が可能で低コスト化が可能な PKI ソリューション
- 電子ビジネスのための連合と協調し、自主規制する認証スキーム「T-Scheme」の策定

2000年4月には、政府のサービスを電子化するという目標を達成するため、そのフレームワーク確立へ向けての電子政府戦略が公表された。戦略は、情報基盤の中央への統合というアプローチと、地方自治

体への分権というアプローチの、両方の利点を最大限にすることを目標とするものである。また英国政府は、方針を進めるうえでは、政府の各部門間の垣根を越え、民間とも協力しながら実施に当たるとした。

電子政府戦略のフレームワークは、認証、相互運用、メタデータ、セキュリティ、スマートカード、プライバシーの各重点分野から開発されている(表2参照)。

## 4. 基盤技術としての T-Scheme

### 4-1. T-Scheme の構成と役割

T-Scheme は、信頼性の提供のために厳密な評価基準を作成し、独立組織の運営により産業が主体となって自主規制するスキームである。

T-Scheme は、「認証プロフィール」と呼ばれる基準セットを構築し、これによって保証を行なうスキームである。認証プロフィールの策定や評価は、一連の T-Scheme の枠組みからは独立しており、選定された参考人によって評価が行なわれる。

表2 英国の電子政府への取り組みにおける重点分野

項目	内容
認証	政府がオンラインサービスおよびコールセンターを提供する際には、その処理が個人やビジネス慣行上で広く容認された手続に則っていることが要求される。認証フレームワークポリシーおよびガイドラインは、政府省庁、税関および公共部門に共通した認証手続を設定。
相互運用	すべての政府省庁および公共部門を横断する相互運用を行う際の、相互運用フレームワークポリシーを作成。
メタデータ	電子政府を運用するための、メタデータポリシー作成が進行中。
セキュリティ	セキュリティポリシーは、安全な電子商取引を実現するために備えるべき、一連の要件を定めている。この適用範囲は公共部門のみでなく、公共事業に係るサービスを提供する、すべての組織にまで及ぶ。ビジネス・サービスやネットワークに求められる信頼性、機密性およびプライバシーなどを含めた、特定のセキュリティ問題についての補足のガイダンスも、近々公表される。
スマートカード	スマートカード・フレームワークポリシーは、相互運用を促進するためのガイドラインを提供する。また公の機関に、任意のカード・スキームとの相互接続性が不可欠であることを説明するとともに、データ保護問題についてのガイダンスを提供。
プライバシー	政府白書では、「プライバシーに対する懸念に取り組み」、そして「データ共有に適切・正当な基礎を供給する(例えば、不正行為縮小のために、改善されたサービスが要望される)」が謳われている。データ共有は、近代化する政府の協議事項の中心となる。

参考: "International Benchmarking Report Summary-UK" (UK online)  
([http://www.e-envoy.gov.uk/publications/reports/benchmarking/summary\\_uk.htm](http://www.e-envoy.gov.uk/publications/reports/benchmarking/summary_uk.htm))

※2 CLOUD COVER プロジェクト … 英国政府における PKI 運用(政府機関への PKI 導入、相互運用性の確保、費用対効果を考えたシステム開発など)の確立を目的とした CESG(政府の情報セキュリティを担当する機関)のプロジェクト。プロジェクトは既に終了している。CLOUD COVER プロジェクトの主な成果は以下の通り。

- ・ 政府機関の PKI 導入(調達)ガイダンスの作成・提供
- ・ HMG Root Authority(政府の最上位認証局)を基礎とした戦略性の高い技術システムの採用
- ・ PKI 製品間の互換性・相互運用性の調査・研究

(参考 <http://www.manaboo.com/webdiary/wd121009gpci.htm>)

T-Scheme による認証は、電子処理に頼る個人および会社に保証を行なうことにより、e ビジネスの成長を促進させる。T-Scheme は、認証サービスを行うのための、認証プロフィールと呼ばれる基準セットを用意している。この基準セットに適合することを実証することができるサービス・プロバイダには、「T-Scheme 認証マーク」の使用を許可するが、これはビジネスへの付加価値を提供する。

#### 4-2. 「自主規制」(self-regulatory)

認証プロフィールは、周期的に調査され、頻繁に書き換えられる。認証システムの稼働時には、参考人によって行なわれた任意の監査と周期的な再評価によって、内容の一致が保証される。

T-Scheme とサービス・プロバイダの間の認証契約では、サービス・プロバイダの是正すべき点に関する正当な苦情や、あるいは過失の場合についても、それぞれの場合に応じた制裁手続きが用意されている。可能な制裁には、即時の修正、怪我をしたものの補償および認証権の終了などが含まれる。それらの義務への違反が見つかった場合については、それらの認証契約で指定される訴訟に関する権利を行使できる。

T-Scheme の運営で、保証によって制限されたものについては、英国政府から独立した非営利法人として成立している。これは、産業、ユーザ、政府、同業組合、消費者グループ、金融機関およびトラスト・サービス・プロバイダおよび技術サプライヤーを含むコミュニティなど、すべてのセクターから予約を通じて会員を求めオープンで中立な組織である。しかし、非営利組織 tScheme は、運営資金を得る目的で、会員予約や T-Scheme 認証、T-Scheme マークの使用などから収入を得ている。

#### 4-3. 認証のフレームワーク

T-Scheme は、特定の組織と特定のサービスとのコンビネーションを認証する。サービスを認証する過程は、次のような多くの個別のステップを含んでいる。

1. T-Scheme は、認証プロフィールの適切な範囲を開発し、認可し、公表する。
2. T-Scheme の使用においては、認証プロフィールに対する監査を試みるため、適切な資格のある参考人を用意する。

3. トラスト・サービス・プロバイダー(TSP)は、プロフィール(複数可)で定義されたサービスを監査するために、参考人から評価報告書を受け取る。
4. TSP は、適格であることを証明する参考人の報告書を引用して、認証者として許可されたことを表すフォームを作成する。
5. T-Scheme は評価報告書を考慮し、もし満たされれば、サービス・プロバイダーの T-Scheme マークの使用および参加者の支払条件をカバーする契約に調印し、かつ認証料金を払うことを TSP に依頼する。
6. T-Scheme は、良いとされたサービスのそのウェブ・ベースのディレクトリーに TSP を加える。TSP は、サービスマークによって、サービスが信頼性の標準に適合していることをそのユーザに示すとともに、T-Scheme との契約期間を表示する。

認証プロフィールは、以下の項目を保持し、適切な状態を保つことを目的とする。

- サービス・プロバイダは適切に設立され、方策に問題はないか。
- サービスは十分に定義されているか。
- サービスは公平か、また合理的か。
- サービスはその定義通りに提供されているか。
- それは十分に安全か。

### 5. 標準技術としての T-Scheme — E コマースの 活性化への貢献

1998 年、英国の貿易構成グループは「トラスト・サービス・グループ(Trust Services Group)」を形成した。このグループは、政府戦略の議案通過の際に大きな役割を果たした。同グループでは、同様のスキームの開発や、英国政府のイニシアチブの下で認証システムを構築することなどを通じて、英国外に向け T-Scheme がさらに発展していくことに大きく期待を向けている。

T-Scheme は、協力と相互評価を拡張する目的でヨーロッパや他の国々を横断し、各国間を等価に結びつける。T-Scheme の目標の 1 つは、多くのトラスト・サービス・プロバイダーが、国際的なコミュニケーションの基礎を築くことである。国境を越えた取引において、消費者や企業間の信用を確保する役割は非常に重要である。

[ 参 考 ]

- 電子商取引推進協議会 『電子政府委員会報告書』 2001年3月  
<http://www.ecom.jp/report/h12seika/egovernment/egov.pdf>
- “欧州における電子署名の標準化”  
<http://www.net.intap.or.jp/INTAP/information/report/h11-sec/1.pdf>
- “Progressive Governance – What is best practice in beating the digital divide?” (UK Government)  
[http://www.progressive.gov.se/dokument/UK\\_Social\\_inclusion.doc](http://www.progressive.gov.se/dokument/UK_Social_inclusion.doc)
- <http://www.ukon4b-humber.co.uk/business/how-to-guides/Being%20Secure.doc>
- “International Benchmarking Report Summary-UK” (UK online)  
[http://www.e-envoy.gov.uk/publications/reports/benchmarking/summary\\_uk.htm](http://www.e-envoy.gov.uk/publications/reports/benchmarking/summary_uk.htm)
- tScheme Ltd ホームページ  
<http://www.tscheme.org/>