嗜好に関する情報の収集・管理。ダイレクトな顧客管理の下での当情報のリリース。
- 複数の対象品から「最も買い得の」価格で日用品を購入できるよう管理（中小企業には文具、国内消費者向けには生鮮品を除く商品など）。
- 商品構成管理と更新管理（購入後のソフトウェア、または保険など）。

売り手側の利点
- 支払いの保証。
- 地方の顧客サービスとサポート。
- 顧客の購買嗜好に関する詳細情報への認可アクセスの付与。対象をきわめて絞った1対1販売とそのフォロー・アップに使用。
- 一般市場開発および動向に関する権威ある匿名扱いデータへのアクセス。

信託サービス・プロバイダ（暗号化サービス・プロバイダ）の認可制度

暗号化、公開キー、および署名としてのこれらの使用方法

専門外の人々に対し理解を助けるという意味で、ここで多少なりとも隠語について説明しておいた方が良いと思われます。電子署名法の1つは、公開キー、または非対称の暗号手法として知られる方法を活用することであります。公開キーでは、キー・ペアとしても知られる2つのキーを使用します（これらのキーは、いずれも特殊な数学的プロパティを持つ同一番号であります）。署名にこの手法を使用する場合、専用キー（名称からわかるように、所有者のみがキーを知っている）が、データ内に収められた情報の波長を変えてデータ・ファイルを変換するために使用されます。こうして変換されたデータが電子署名であります。署名した人物の公開キーを使用すると、元ファイルとこの署名とを照合することができます。公開キーにアクセスできる人物であれば誰でも署名を照合することができるため、専用キーへのアクセス権を持つ人物だけがこの署名を行うことができたことを確認できます。専用キーへのアクセス権を持つ人物だけが署名捺印者であれば、この捺印者がメッセージに署名したことは間違いなく、署名の事実を後になって否定することはできません（否認）。仮に、第三者がこのメッセージを変更したとしても、この第三者が犯した事実を難なく検出することができます。

機密性について

メッセージや保存データの機密保持にも、冒頭で説明した公開キー暗号化を使用することができます。メッセージの送り手は、受信相手の公開キーを受け取り（署名と機密保持には通常、別のキー・ペアが使用されます）、このキーを使用してメッセージの波長を変えます。これを解除するには、対応する専用キーだけが使用されます。これが、公開キーを使用してメッセージの波長を変えた受信相手側がメッセージ解読時に行う処理です。対象となる受信者の専用キーへのアクセス権のない第三者は、メッセージを解読することはできません。

33. 電子署名および書込を法的に承認するほか、電子商取引を活性化するには、より多くの実践が要であると政府は考えています。電子署名は、確実に情報を保全し（つまり、内容に変更が加えられなかったことを保証し）、この情報の作成者を確実に照合するために使用できるものです。このほか、インターネットのように門戸開放型のネットワークを使用する人たちが特に懸念することとして、機密保持（電子的に送信された情報の機密保持）

が挙げられます。しかしながら、この技術は複雑なうえ、多くの人々にとってなじみが薄いものです。機密保持の安全性を可能にする技術と、この安全性を提供する商業団体のいずれもがユーザーからの信頼を勝ち得るには、政府の果たす役割が重要であります。したがって、社会への暗号化サービス提供団体に対して任意の認可制度を導入すれば、信頼が確立されるため、品質とサービスの最低基準を確実に満たせば市場は活性化されます。機密保持サービスが社会において広く普及し、特に「開放型」取引に活用されるためには、ユーザーは先ず高いレベルの信頼を求めるものと考えます。ここで求められる信頼レベルは、銀行または弁護士に要求されるような水準と思われます。銀行または弁護士が提供するサービスのように十分定着したサービスは、規制を受けており、これらのサービスは信頼に値するという長年に渡って培われた安心感から信託を受けているのです。電子世界においてこうした信頼を事実上一夜にして確立するのは並大抵のことではありません。しかしながら、政府認識としては、ライバル間ですでに信用が存在し、プロバイダーの「信用」がそれほど重要ではなさそうな「閉鎖型」環境においても、電子署名と暗号化が提供されることになると考えられます。このような理由から、政府としては法定制度ではなく任意制度を選択いたしました。

34. 本セクションでは、当該認可制度の機能に対する政府側解釈について詳述します。しかしながら、第一次立法には本詳細の一部始終が盛り込まれることにはならないと思われます。したがって、その目的は、第一次立法によって、本詳細の導入手段となる第二次立法（委任立法集）繰り上げのための政府権限が付与されることにあります。言うまでもなくDTIでは、今後も引き続きこうした詳細の諮問を欠かさない所存であります。認可条件に関するDTIの当初の意向については添付資料Aに収められています。また特に、この添付資料に関するご意見については、積極的にお寄せいただきたいと考えております。

35. 英国政府は、電子署名と暗号化を明確に区別する政策をお約束しています。この政策には、前行政が打ち出した諮問の過程において業界が表明した根拠の確かな懸念事項が反映されています。またこの政策では、電子署名と暗号化サービスを商業的に利用する各種の形態や、それらが政策に提示しているさまざまな課題も認識されています。署名と暗号化の主な違いは、以下の通りであります。

- ライセンス認可機関では、キー・ペアのうち、電子署名を目的としてのみ発行される専用キーを保存することができません。したがって、専用署名キーの保全責任は紛れもなく所有者本人にあります。こうした手続きでは否認が回避されるため、電子署名に対する信頼が強化されると考えられます。

(ページ19)

- 機密保持目的に情報を暗号化するときに専用キーを使用したことがなくても、（専用

キーが保持される場合にはいかなる場合にも）法執行機関が署名用の専用キーにアクセスすることはありません。

- 署名サービス・プロバイダと機密保持サービス・プロバイダ間の認可基準（添付資料A を参照）は明確に区別されます。

36. 機密保持または暗号化の提供団体、または保存データや送信データ内容保護のために暗号化を使用するサービス（つまり、キー管理サービス）提供団体にも認可制度を適用した方が望ましいと思われます。企業では、スタッフの手により暗号化された重要データや、クライアントに送付したメッセージ文を復元できることが重要であるという認識がますます高まっています。過失にせよ、従業員が置き忘れたにせよ、暗号キーを紛失するようなことがあれば、企業は大きな損害を受けることになります。したがって機密保持サービス・プロバイダーは、適切な保管協定またはキーの隠ぺい商品を使用して、キー（つまり、情報機密性保安情報）の復元を可能にするよう奨励します[17]。

37. こうした技術が普及し配備されると、厳格な規制手続きに基づいて法執行機関が暗号キーを復元することができ、法の執行もサポートされることになります。暗号キーの使用を英国政府は奨励すべきである、あるいは命令すべきであるという声さえ聞こえてくるなかで、それにも勝る論陣が国内外で張られていることを政府は十分に承知しています。暗号化技術の実用性、コスト、望ましさについてはさまざまな見解があるため、政府としては、第三者へのキー委託と第三者によるキーの復元のいずれも、機密保持サービスの許認可要件からはずす基準で諮問するという結論に至りました。機密保持サービスの利用者は、こうしたサービス利用の是非をみずからの意志で自由に決断することができます。暗号化の利用者がキーを保管する必要はないが、機密保持用のキーを紛失するようなことになった場合、備えのない人はデータ紛失のリスクを背負うことになります。

38. 本書ではこれまで、署名サービスと機密保持サービスという二つのサービス・タイプ

脚注[17]：委託を受けた第三者(TTP）や、第三者へのキー委託を使用する代わりに、キー復元（キー隠ぺいとも言う）をサポートする暗号化商品を使用します。（紛らわしいが、キー復元とは、キーの保管つまり「第三者へのキー委託」と、キー隠ぺいという二つの言葉に適用できる一般用語として使用できます。本書では、キー復元と言う言葉のみを狭義に使用します)。こうした市販の暗号化商品は、すでに米国で用いられているもので、キー復元業者（KRA)として知られる代理業者（通常は、企業）の公開キーをこうした商品には組み込むことができます。これにより、暗号化商品の利用者は、メッセージの暗号部分からKRA にアクセスし、保存データや通信データを復元することができます。書面による認可がKRA で降りていれば、（メッセージごとに異なることが多い）キーへのアクセスは法的にも可能であります。利用者によるアクセスと、法執行機関によるアクセスのいずれの場合においても、KRA が利用者の専用キーを保管することはなく、暗号化を施す前のデータ内容にアクセスすることもありません。

を集中的に取り扱ってきました。任意認可制度では、キー復元業者（KRA: 脚注[17]を参照）も対象としています。政府提案では、暗号作成サービス市場の活性化を計画していますが、対象は暗号作成サービスやその技術的導入、あるいは特定の事業モデルだけにとどまるものではありません。以下のボックスに示した制度のもとで現実に認可を適用できるサービス例をいくつか示します。提示例は例証であって規定ではありません。

（ページ20）

政府では、提示例についてご意見を積極的に求めております。また、各団体が暗号作成サービスを社会に提供するための事業モデルをさまざまに考慮していることも認識しております。暗号作成サービスと認可制度が調和していくにはどうしたらよいか、お考えをお寄せいただきたいと考えております。

暗号作成サービスの実例

電子署名を行う一つの方法は、非対称の暗号作成手法（17ページのボックスを参照）を利用して、専用キーでメッセージに署名する方法です。メッセージの受信者は、対応する公開キーを使用してメッセージを照合できます。本書では、水面下にあると思われる多くのサービスを含める意味で、**認定機関**（CA）という用語を使用します。 「不可価値」サービスも二次的に発生する可能性があります（以下を参照）。認定機関のサービスは以下のとおりであります。	
登録	目的のいかんにかかわらず、公開キーの認可を適用する人物の信用証明書を照合します。この信用証明書には、特に認可対象者の身元証明または属性チェックが含まれます。
認定	認定書を発行します（登録プロセスの一環として）。公開キーが指定所有者のものであることを保証します。
キーの作成	認定書の発行に合わせてキー・ペア（専用キーと公開キー）が生成されるプロセスの最重要部分であります。
認定取消	認定には、失効、変更、専用キーの不正公開、または認定所有者による契約違反など、さまざまな理由で取消が必要になることがあります。取消が行われると、当然ながらこのサービスの一環として、認定機関またはその代行業者によって当該認可に関連する全ての人々がその事実を適切に利用できるようにします。通常、このプロセスには公開リストにより認定取消が明らかにされます。
以下の提供機関に対しても認可を利用することができると考えられます。	
ディレクトリ・サービス	パブリック・アクセス・レジスターの確立。これにより、（署名または機密保持のいずれかに対する）公開キーが安全に保管され、取消情報は更新されます。

タイム・スタンプ	特定の電子文書が存在した証拠を提示するサービス。または、特定時間になんらかのイベントが発生したことを示すサービス。

39. ライセンス供与体制がカバーできる業務範囲を指定すると、企業がライセンスに規定された範囲内と範囲外でも業務を拡大したいと考えるようになったときの混乱をどのように避けるかという問題が浮上してきます。オプションの一つは、ライセンス供与体制でカバーされた全ての暗号化業務のライセンスを持った企業に対しては、その企業がオファーすると決定した暗号化業務全てにライセンスを供与すると要求することです。

（ページ21）
このようなアプローチは電子商取引が急速に発展した場合には、新規の付加価値のある業務に対する改革や発展を抑えることになり、柔軟性に欠けることになるかもしれません。任意のライセンス供与体制の精神に反すると反論する人もいます。しかし、特定の暗号化業務の品質に関して消費者を混乱させるようなメッセージを送信しないようにすることが重要です。**従って、政府は、消費者を守るためにライセンスを持つ業者とライセンスを持たない業者によるサービスをいかにうまく分けるかという点に関するご意見をお待ちしています。**

ライセンス供与機関

40. 政府の意向では、ライセンスの発行、変更、およびライセンス供与条件への準拠の監視権限は貿易産業大臣との協議によるということです。国務長官にはその権限の一部を、必要に応じてその権限を別の委任可能な人に委譲できる権限があります。政府は権限の委任については詳細に検討した上で、権限を全て委任するのではなくライセンス供与の一部はそのまま残すことになるでしょう。

41. 任意ライセンス供与体制を設定したときのキーとなる目的は、消費者の間にライセンスを持った企業は信頼できるという確信を持ってもらうことでした。従って、ライセンス供与のフレームワークは厳格なもので、公明正大で、全産業界から信頼される必要があります。法令によるアプローチを選択した理由はここにあります。政府の認識では、各業界の自主規制によって業務がなされ、その業務を法令の枠組の中に組み込むことを望んでいるということです。しかし、この仕組みはまだ未発達状態にありまだ機能しておらず全ての業界の支持も得ておりません。従って、個人の申請者に対する業務の一部は機関外へ委任されることはあるにしても、法的機関がこの任意体制を監視するのが適切と思われます。政府は認可機関第１号として OFTEL を指名することを決めたようです。DTI ならびに OFTEL は業界と緊密に連絡を取りながら業務を進め、ライセンス供与された機関が準拠

できるような基準の開発に取り組みますが、消費者の信頼を獲得するという目的は、その基準に準拠した法の執行をする法的機関を設立することで達成されるはずです。事実、OFTEL もライセンス供与機関としての機能を業界に委任することを考えているようです。政府は、将来ライセンス供与機能の一部または全てを委任することを禁止しないようです。

保証

42. **政府の認識では保証問題が業界にとってのキーとなる関心事であるため、本セクションに提示された問題に関するご意見を特にお待ちしています。**電子商取引の世界における保証は複雑で、政府は直接であれ間接であれ特定の取引に関与するさまざまな関係者の利害のバランスをとる必要性を認識しています。原則は政策は技術的に中立であり、電子世界での保証は出来る限り伝統的な世界と一致するべきということです。しかし、紙とペンによる取引の世界には暗号化業務に直接類似したものはないため、特別なルールが必要になるのです。**一般的な質問は次の通りです。**

- **特別な法律が必要ですか。**

（ページ 22）

- **法律は保証についてどこまで規定するのですか。**
- **法律は第三者が依存する保証体制を契約書、証明書、その他の法律文書の中に言明するよう特別な要求を課すのですか。**

ライセンスの有無にかかわらず、全ての暗号化業務のプロバイダーに課せられる最低限の保証レベルはどのようなものですか。

43. 最低限アプローチはサービス・プロバイダーと顧客間の契約のみに依存します。しかし、この方法はサービス・プロバイダーに全ての保証を放棄して電子署名に依存している第三者を全く保護しないというオプションを与えることになります。いずれにしても、現在の EU 指令のドラフトでは、認可機関は、当局が発行する認可証明書 [18] に正当に依存している人に対してそこに記載されている内容の信ぴょう性について責任があります。**そこで、政府はライセンスを持たない認可機関が負うべき保証（負わなければならない場合）のレベルに関するご意見をお待ちしています。**政府の考えは、既存法の保証に対する規定は他のライセンスを持たない暗号化業務のプロバイダーの責任を十分カバーしており、新たに特別な要件は必要ないというものです。

ライセンスを持った暗号化業務のプロバイダーにはどのような保証体制が適用されるべきですか。