90. 英国政府は法執行機関の必要性が既存のおよび今後の暗号化と通信技術の開発に合致できるかという面から、業界よりのご意見をお待ちしております。

(ページ34)

付録 A　ライセンシングの基準

本付録Aでは、英国政府がライセンス申請を査定することを目的として使用する基準の草案を記載します。提示された基準は、ライセンスが申請された業務の内容により変わるものであり、署名サービスのプロバイダーや機密保持サービスのプロバイダーなど最も一般的な業務であると最初に予想されるものに対しては追加基準をつけ、すべての業務に対して設定されています。この基準は、他の暗号化業務にも広く適用されているライセンシングの管理形態を排除するものではありません（たとえば、タイムスタンピングサービスなど）。政府は、管理形態は必要性が発生した時点で、また技術の発展に伴い別のサービスも組込むことができるように十分柔軟性のあるものにしておくべきであると考えています。

これらの基準は法制化される前の二次的なものです。法制化前に今検討される理由にはふたつあります。第1に法制化が強力な充分なものになること。第2に将来の申請者が基準を満たしていることを確実にするためです。

ライセンシング基準案

(I)　一般のライセンシング基準

次の基準は、すべてのライセンスされた信託業務プロバイダーに対して適用されます。

<u>所有者および役員管理者は適正、的確な人材とします。</u>

管理者がサービスの提供を行うに足る者であり、すべての観点から資格に適した者であること（たとえば、役員管理者として）を申請者の義務として証明するものとします。

<u>英国内の登録事務所</u>

通信文書の送り先となる英国国内の事務所の住所（「看板」のみの住所ではなく）を記載する必要があります。ライセンシーは組織を運営している責任者とリアルタイムで通信するための規定を必要と望んでいます。

<u>雇用者の詳しい調査</u>

プロバイダーは、すべての雇用者、特に潜在的なクライアントと接触する雇用者すべてに

ついて、詳しく調査する（犯罪経歴など）ための適切な手順を準備するものとします。

組織の財務の独立性

プロバイダーは、一般には財源と必要な場合には財務の保証人を示したビジネスプランを作成するなど提供したいサービスを行うための適切な財源を所有していることを証明する必要があります。

ビジネスプラン

財源を示す他に、申請者はビジネス戦略を詳細に示したプラン、市場で生き残るための能力、およびあるかもしれない市場から撤退する場合の方法などの緊急時プランを作成することが要求されるものとします。

(ページ 35)

エージェント

状況によって、業務は複数の組織によって履行されることが認められます。このような場合には、申請者とどのような契約関係にある組織かを示すとともに、エージェントに関する詳細説明を提出する必要があります。

品質管理

申請者と、必要な場合にはその主要エージェントは、ISO 関連条項など、適切な品質システムの関連条項に従うことを証明する必要があります。

情報セキュリティ管理

プロバイダーは、BS 7799 (c:cure スキームに基づいて) に信任状の入手、または少なくとも信任状を提出するように求められるものとします。

保証債務

本書 21 ページに記載される可能な要求には関係なく、申請者はクライアントまたは第三者と締結したい債務に合致する能力（すなわち、十分な財務資源）があることを証明する必要があります。

データ保護

申請者は、(カスタマデータに関し) データ保護法 (1998) 及びその他の法令の規定に従うことを証明するよう要求されるものとします。

キージェネレーション

申請者は、署名及び機密保持サービスのため、別のキーペアを発行できることを証明するものとします。

(II) 証明権限に対するライセンシングの基準

技術的保証

プロバイダーは、必要に応じて、キーペアの作成および専用のプライベートキーの保存に使用するシステムを、セキュリティ保証の面から独自に判定できること (たとえば、ITSEC または CC 認証[20] の発行により) の証拠を提示するものとします。

認証内容

申請者は、発行する認証には以下の情報が入っていることを証明する必要があります。

- サービスプロバイダーの身元証明
- 所有者の名前、または同意された雅号
- 所有者特定の属性（たとえば、住所または財務状態）
- 認証の有効期間
- 独自の認証番号
- 情報の機密保持を確実に守るために使用されているキーを有効にするために認証が使われてはならないことを明確に示した記述
- 認証使用に関する特定の制限 (すなわち、使用可能なトランザクションの他に制限される場合など)

---

[20] ITSEC または共用基準認証は、製品が特定のセキュリティ保証基準に合致するものとして査定され、認められた認証団体に発行されます。このような製品を査定するためのスキームは、ドイツ、フランス、アメリカ、カナダ、英国にあります。

(ページ 36)

- 発行する CA の身元保証

キーペアの生成

プロバイダーは、非対称のキーペアを作成し、必要な場合には、それをクライアントに配送する方法を詳細に示したものを提出する必要があります。キーペアがクライアント生成のものである場合は、使用する生成プロセスの詳細を提示する必要があります。

プライベート署名キー

申請者はプライベート署名キーが、確実に対象のクライアントのみに知らされるようにするためのメカニズムの詳細を提供しなければなりません。指定所有者以外の任意のものにキーを開示することはライセンス違反となります。

クライアントの認証

申請者は、そのクライアントを認証するために使用する予定の手順の詳細を提示することが求められるものとします。この提示を行う際には、CA あるいは契約締結されているエージェントによる事前の物理的確認（たとえば、登録権限など）が必要です。

取消し

申請者は、迅速で、かつ、わかりやすい取消しサービスを提供するための適切なシステムを所有していることを実証する必要があります（公共の書式を使用して）。

ユーザー署名生成製品

ライセンス条件ではないが、ライセンスされた認証権限を持つクライアントは、完全な法的認定 (12 ページを参照)の利点を活用するときには、「認証された」署名生成製品を使用しなければなりません。「認証された」製品の情報を提供するときには、このライセンスされた認証権限が必要となります。

(III) 機密保持サービス規定に対する TTP の条件

キーの保存

キーが保存される場合、申請者は、そのクライアントの暗号化されたキー（またはその他の適切な情報）を安全に保持する能力を有していることを証明できなければなりません。このような「セキュリティー」には、セキュリティー保証の観点から独立してアクセスできる（たとえば、ITSEC または CC 証明の発行などにより）コンピュータなどがあります。

法的有効アクセス

申請者は、ライセンス条件に指定される期間内に有効化された署名による認証に応えるため、所有している適切な情報 （たとえば、ユーザーのプライベート暗号化キーまたは他の関連情報）を作成するため技術的方法及び手順を整えておかなければならないものとします。

アクセス要求の認証

TTP はキーに対する要求を認証するか判断する手順および権限のない要求を拒否する手順を確立しておくものとします。

---

[21] 12 ページの脚注を参照。

(ページ 37)

(IV) キーリカバリー エージェントの条件

法律の強制執行との関係

ライセンスを受けるため申請しているエージェントは、適切な権限を持って提示された場合に、法執行機関に対し適切なキーリカバリー情報を電子データで提供できることを実証しなければなりません。

アクセス要求の認証

キーリカバリーエージェントは要求の認証を判定する手順および権限なしの要求を拒否する手順を確立しておかなければなりません。

これらの基準に対してのご意見をお聞かせください。また標準規定を設定すべきレベル、およびどのように査定すべきかなどについてのご意見もお待ちしています。英国政府が意向とすることは、高いレベルでの消費者保護を確保し、一方でライセンスされたサービスの提供者に不要な負担やコストをかけないようにするため、このサービス市場にとって本質的となるような信託業務を構築していくことです。

(ページ３８)

付属文書 B -- 用語集

本付属文書および主文書内のボックスおよび脚注は専門用語のガイドとして提供いたします。法的な定義付けとしては信頼性に欠ける場合があります。

Authentication（認証）

要求した身元の確認。

Certification Authority (CA) (認可機関)

認可機関とは電子署名と特定の個人または企業をリンクするための証明書を発行する委託

業務プロバイダー（TSP）(20 ページのボックス参照) 。

Confidentiality （機密保持）
情報を機密に扱うこと。

Cryptography （暗号化）
メッセージの安全性を保持する方法または技術。

Electronic signature （電子署名）
手書きの署名の電子版に相当する電子文書と関連付けられたもの（4 ページおよび 17 ページのボックス参照）。

Integrity （保全）
保全を確認するとは情報の内容が権限なく変更されることを防ぐことを指す。

Key escrow （キー・エスクロー）
委託第三者（TTP）によるユーザーのプライベート秘密キーの保管で、暗黙の取り決めにより取り出せるもの。例えば法執行などの目的で定義した取り決めに基づいて取り出せる。

Key recovery （キー復元）
権限を持った個人が特定の条件に基づき暗号化されたデータを複数の関係者の情報を得ながら解読できる機能。

Key management (キー管理)
暗号化キーを管理（作成、保管、配布、変更、取消しなど）するプロセス。

(ページ３９)
Key revocation （キー取消し）
公開キー（目的を問わず）が無効になったという通知。

Plaintext （プレーンテキスト）
暗号化される前のオリジナル データ。

Private Key （プライベート・キー）
暗号キー・ペアのプライベート（秘密）部で、厳重な管理がされるもの。

Public Key （公開キー）
暗号キー・ペアの公開（非秘密）部。このキーは公開されており秘密部を添付する必要はない。

Qualified certificate （認定証明書）
EU 電子署名指令の付属書類 I の要求に準拠し、認可当局（ライセンスの有無を問わず）が指令の付属書類 II に準拠している署名証明書。

Trust Service Provider (TSP) （委託業務プロバイダー）
暗号化業務を行うプロバイダー（ライセンスの有無を問わず）の総称（5 ページの脚注 [3] および 20 ページのボックスを参照）。

Trusted Third Party (TTP) (委託第三者)
秘密のキー管理業務およびキー・エスクローを提供する特殊タイプの委託業務プロバイダー。