44. ライセンス供与体制の目的はライセンスを持ったプロバイダーに対する信頼をつくりあげることです。ライセンスが与えられていることで、サービスの質が高度であるということを一般大衆が確信できるようにする必要があるのです。競争的需要をバランスさせるという明確なニーズがあります。

- ライセンス・サービスの購入者は、ライセンスによって何か品質面での保証がされることを期待します。例えば、顧客は署名キーのペアを作成する際には十分な注意が払われることを期待し、機密サービスを購入する人は TTP にプライベート秘密キーを保管してもらう場合には適切な注意が払われることを期待します。
- ライセンス/サービスに依存する第三者は同様な期待をします。例えば、証明書に記載されていることが事実で、その内容に偽りがあった場合は認可機関には何らかの責任があり、ライセンス取り消しなどの有効な対策が取られることなど。
- サービス/プロバイダーは、自己の責任の管理および制限ができる必要があり、ライセンスの供与を受けることが無制限の責任を負うということを意味する場合はライセンスの申請はしません。保証に上限を設けるとライセンスを受ける際の保険料が下がるという利点はあります。

45. 政府の当初の考え方は、これらの競争的需要は保証 [19] に制限を設けることで折り合いをつけることができるというものでしたが、ライセンスを持ったサービス・プロバイダーの契約条項により保証の範囲を下げることはできません。サービスの内容により異なる保証レベルが設定されることになります。顧客はライセンスを持ったプロバイダーは特定のレベルの保証を負ってくれるという認識で保護されるのです（もちろん、ライセンスを持ったプロバイダーはより高レベルの保証をオファーするのは自由です）。プロバイダーの権限もその保証範囲に限度を設けることで守られています（保証の限度は、商売上の利益が確保できるのであれば上げることもできます）。

脚注 [18] ： 脚注 [14] を参照。

脚注 [19]： EU 電子署名指令は現在では保証の金融的制限は設けていません。
政府はこのような制限が英国立法に追加される前に、指令と一致していることを確認する必要があります。

（ページ 23）

政府はこのアプローチに関するご意見、どのように保証制限を設定するのか、またはこれに代わるアプローチのご提案がありましたらお待ちしております。

プライベート・キーの所有者にも特定の「注意を払う義務」を課すべきでしょうか（プライベート・キーの安全性の保持やプライベート・キーの暗号化が解除されたら何時間以内に

認可当局に通知する必要があるなど）。

立法化の際に強調する必要がある暗号化業務に関する責任問題が他にありますか。

ライセンス料

46. ライセンス料はライセンスの申請、ライセンス供与後の監視、ライセンス条件に実施の確認などに要した時間に応じて、即ちライセンス供与機関のコストをカバーして設定されます。ライセンス料はライセンス供与機関によって設定されます。作業に要した時間により料金は異なり、サービスの内容によっても異なります。

輸出管理

47. 提案している立法それ自体は、国際協定によって決められている暗号化製品の現行の輸出管理に影響は及ぼしません。しかし、第三者を通じた合法的なアクセスを促進する暗号化製品（キー保管とキー復元を組み込んだ製品など）の輸出手順の合理化ができそうです。これを実行する方法の一つは、包括輸出許可制のもとで一度の見直しの後に設定基準に合格した製品の輸出を許可するというものです。

暗号化に対する警察の関与

48. 暗号化は貿易、産業界、個人に明らかに恩恵をもたらします。例えば、銀行は支払システムや現金自働支払機で暗号化に依存しています。暗号化はインターネット上での犯罪防止にも役立ちます。例えば、企業や個人から財産をだまし取ることがかなり難しくなります。また、暗号化を使用して知的財産を守ることができます。ただし、犯罪者は新しい技術を利用するのが早いため、麻薬密輸業者、テロリスト、小児愛者などの深刻な犯罪者が捜査当局を打ち負かすことを目的に暗号化を利用することは間違いないことでしょう。事実、こういうことが発生しつつあるのです。従って、政府はビジネスやその他での暗号化の合法的な使用の促進と助長と、犯罪者による使用を出来るだけ難しくするという二重の責任を持つことになるのです。

警察に対する暗号化の脅威

49. 最近の英国におけるさまざまな深刻な犯罪の調査において、本来は調査の手助けになるであろう材料や証拠として使用された材料が暗号化されており捜査の妨げになっています。この種の問題は増加しています。

(ページ 24)

捜査当局はしばしば暗号化キーの「解読」を試みます。時々多くの時間と費用を費やして成功することもありますが、不可能ではないにしても技術の進歩とともにますます難しくな

っています。

50. 次の例は問題の本質を示したものです（この他にも、審理中のものを含めさまざな理由により公表できないものもあります）。

罪：

- 1998 年、殺人未遂およびレイプに対する警察の捜査は容疑者のコンピュータで暗号化された資料が発見され妨害されました。容疑者から押収されたその他のものの中から警察が関連暗号化キーを発見するまで、警察の捜査は進行できませんでした。
- 小児愛者が暗号化を使用して警察当局の目から自分達の非合法な行動を隠そうとするケースは数多くあります。例えば 1995 年、インターネット上で子供のポルノを配信していたという容疑で 2 人の小児愛者が英国の警察に逮捕されました。コンピュータ・システムに子供のポルノ画像があることが発見され、主犯容疑者の場合には大量の暗号化資料が発見されました。調査によると、容疑者は暗号化通信を利用して子供のポルノを世界中の関係者に電子メールで配信していました。その後、二人の小児愛者は子供のポルノ配信の罪で有罪判決を受けましたが、主犯容疑者に対する警察の捜査は暗号化を使用していたということで大変な妨害を受けました。

詐欺および金融犯罪：

- 重大詐欺を取り扱う最近の調査では、取り扱ったケースの約 50% で何らかの暗号化が発見されています。さまざまな複雑な暗号化によって保護されたコンピュータ・ファイルのインスタンスが最近の一連の調査で発見されています。 問題の発生は増加しており、暗号化に対処するために他で利用できるはずのさまざまな資源が費やされています。
- 商業権益が不当な暗号化の使用による脅威に直面しています。企業スパイやインサイダーによる窃盗に関わっている人間は、当然その行動を隠すために暗号化デバイスを使用しています。暗号化されたウイルスをコンピュータ・システムに侵入させて企業から金を奪い取るというケースが発生しています（いわゆる暗号強盗）。警察当局に関連暗号キーを取得できる権限があればこの主の犯罪捜査は容易になったはずです。

（ページ 25）

テロリズム：

犯罪を隠すために暗号化を使用したテロリストの例はすでに英国であります。1996 年の終わりに、北アイルランドのテロリスト・グループの中心メンバー数人が逮捕されたことで警察の捜査活動は頂点に達し、暗号化ファイルが搭載されたコンピュータ機器が押収されました。このファイルには警察官や政治家など、テロリストの潜在ターゲット情報が格納されていました。最終的にデータは検索できましたが大変な努力を要しました。

(ページ26)

国際的例

以下の例は犯罪者またはテロリストによる暗号の使用が地球規模の問題になっていることを例証します。

・ 米国において、FBIはRamzi Uousef(1994年の世界貿易センター爆破事件の首謀者で、1995年後半にマニラ航空機を爆破)のラップトップコンピュータに米国の11社の旅客航空機を爆破するというテロ攻撃の計画書に関する暗号化されたファイルを発見しました。

・ 日本では1995年3月に死者12名負傷者6000名以上を出した東京地下鉄サリン毒ガス事件を起こしたオウム真理教が、その記録を暗号化されたファイルに残していました。当局は発見したファイルを解読することができ、発見した証拠は捜査に重要な役割を果たしました。

FBI長官は、かつてこう言いました。
「暗号解読の問題は、犯罪捜査に関連した最も重要な問題のひとつです。そして国家安全に対するあらゆる脅威と戦う我々の能力について、悲劇的な結末をもたらしかねない問題です。法の執行者は、強化された回復不可能な暗号が広く使われることは、犯罪やテロと対決する我々の能力を最終的に破壊するかもしれないと意見が一致しています。」
1998年1月28日　諜報活動に関する「上院選択委員会」での発言

政府の回答

51. 政府は既存の法律の有効性を維持する義務があり、既存の法律は、法の執行、安全保証や諜報機関が犯罪や国家の安全にたいする脅威と対決するのを可能にします。新しい技術(特に商用の暗号化システム)はこれらの機関に対しては新しい挑戦となっています。単純な解決法はなく、政府の回答には3つの重要な要素があります。既存の法の権限を更新する、暗号が広く使われていることを考慮に入れる、キーエスクローの活用とキー回復の技術を奨励し、産業界や関心を持っている団体などと共同して、法律から逃れたり、国家の安全に脅威をもたらす者達が暗号化を使う効果を少なくする方法を見出す。

言い尽くされた神話

52. 政府の提案に関する神話を追い払うことには価値があります。

・ 通信を暗号化するときに、ビジネス社会や個人にキーエスクローやキー回復技術を使用

するように強制的な必要条件を押し付けることはしません。
・ 市販されているどんな暗号化製品を使うかは、個人や企業の自由です。
(ページ27)

・ 技術的に中立で、法の執行者、国家安全、諜報機関の侵略的な監視の力を及ぼしません。提案の目的は、ただ既存の法律の有効性を維持することです。「解読」の権限は暗号化された情報へのアクセスが、既存の法律ですでに獲得されている場合にのみ適応されます。

既存の法律を更新する必要

53. 政府は広く使われている暗号化は法の執行者、国家安全、諜報機関の既存の法律の枠組みの有効性を危うくするものではないこと確認しようと、決心しています。しかし、それが政策の限界です。政府は、あたらしい手段を使って個人の権利を侵害する監視の権限を直接あるいは間接的に拡張するつもりはありません。逆に、新しい権限には強力な保障条項が盛り込まれており、暗号化キーへの不正なアクセスを防止します。

54 暗号化には既存の法律に対する脅威となる、2つの領域があります。通信傍受と捜査と差し押さえの法的な権限。

通信傍受法1985年

55. 1985年の通信傍受法(IOCA)では、公共の電気通信ネットワーク上で通信(電子メールを含む)を傍受するには国務大臣の署名がある令状が必要です。傍受は、国家安全上の観点、重大な犯罪の発見と防止の目的、健全な英国経済の保護の目的に必要とされる場合のみ認められます。他の方法では入手できないと思える合理的な理由があるばあいに、国務大臣は情報の傍受を承認します。法律の実施を監督し、苦情を調査する Commissioner and Tribunal(長官および法廷?)の条項など、法律には数多くの保護策があります。

56. 通信の傍受は、重大な犯罪や国家の安全に対する脅威と戦う重要な道具でした。進行中の捜査を妨げないため、長い間、傍受の詳細内容を公表しない方針でした。次の数字から既存の権限の価値が伺える。1996年から1997年の間に、合法的な通信の傍受は、警察やHM 税関の捜査で時として重要な役割を果たし、次のような結果を得ました。

・ 逮捕者1200名
・ 約3トンのAクラス薬物、112トンの他の薬物を押収、合計の末端価格は6億ポンド以上。
・ 450丁の火器の押収。

同期間で、約 2600 件の傍受の令状が内務大臣により発行されました。(Interception Commissioner (傍受長官) の働きとともに、この数字は警察や税関だけでなく、内務大臣が発行したすべての令状を示します。)

(ページ 28)

57. 政府は既存の傍受法の見直しを決定し、1998 年 9 月 2 日に内務大臣は下院で次のような発表をしました。

「この 10 年間に、電気通信の技術で大きな変化が起こり、Strasbourg にあるヨーロッパ裁判所の決定とともに、命令の制度を新しく考えています。今日、議会に発表できます。この夏の初めに納得のいく傍受制度の見直しに着手しました。近日中に本件に関する助言の文書を発行します。」

58 傍受法の見直しは進行中です。本書の目的は、より幅広い結論を先取りすることではありません。しかし政府は、既存の傍受の制度の有効性を保護するために、今行動を起こす必要があります。暗号化はコンピュータファイルおよび電子メール通信の秘密を保護するためだけに使われているのではありません。正しい装置を使って、電話での会話を暗号化することも可能です。電話とコンピュータ技術を収束すれば、暗号化された会話やデータをネットワーク上で送信することも容易になります。よって傍受機関に通信を解読する権限を導入することは必要です。これは暗号化キーに合法的にアクセスする権限を与えることを意味します。このような権限なしには、暗号化が幅広く使われているので、法の執行者、安全保障や諜報機関に対しては価値ある合法的な道具であるので、傍受の有効性に対する脅威になります。

捜査および差し押さえの権限

59. 1984 年の Police and Criminal Evidence Act (PACE 警察および犯罪証拠法)のもとで、警察は捜査令状を裁判所に申請できます。それにもとづきに、令状に記されている場合あるいは犯罪の証拠と疑う合理的な根拠があるばあい、または犯行が行われた結果得られた場合、保管されているデータも含めて書類を差し押さえできます。PACE には裁判所がそのような資料を提出するように命令する権限も含まれます。同じような権限は他の法律にもあります。(例えば、テロ防止法など)

60. PACE は警察が司法によって権限を与えられていなくても、ある状況では捜査および差し押さえの権限を与えていることを認識することは重要です。(例えば、逮捕後の家宅捜査の権限と逮捕時の捜査権限)

61. PACE には、警察がコンピュータ処理された情報を差し押さえする助けとなる条項があります。PACE の 20 節には法律に基づく権限により、建物内に入った警官に与えられた差し押さえの権限は、コンピュータ内の情報をその場所から、見ることができ読み取れる形で持ち出せるような状態にするように要求する権限と解釈されます。(PACE の前後のどちらでも通過した法令にあるすべての法律を含みます。)

62. 実効的に、警察はコンピュータ処理された情報を見て読み取れる形で提出するように要求する権限がすでにあります。しかし、これは必ずしも警察に差し押さえられた資料の暗号化キーを開示するように要求する明確な法的な根拠を与えるものではありません。建物に入り、コンピュータ処理されたファイルを差し押さえる合法的な権限はあるかもしれませんが、暗号化は、もはや警察がファイルの内容を読むことができないことを意味します。

(ページ 29)

63. 政府は、警察が暗号化キーの開示を要求し、捜査および差し押さえする既存の法的権限の有効性を維持するために、新しい権限を確立することは必要と考えています。これは捜査当局に情報を差し押さえる新しい権限を与えません。微妙な問題のある資料(例えば、法的な特権に関わる資料、通商、ビジネス、専門的職業、報道関係の資料、極秘の医療情報など秘密扱いになっている個人的記録。) へのアクセスについての PACE の附則の保障条項を害することはありません。

実世界での例を使って説明すると、証拠の資料が入っている鍵のかかった金庫を思い浮かべてください。建物の占有者または出入りを許可する人が、立ち入りを拒絶した場合に、捜査の権限のある警官は合理的な権利を用いて金庫を開けます。警察が鍵のかかった金庫をこじ開ける必要があるときに、そのようにできない状況を想像することは難しいです。暗号化された証拠資料の入ったコンピュータを差し押さえても解読することができず、中の資料を調べられないことは、ますます多くなってきています。このために、新しい権限が必要になってきました。

立法の提案

64 政府は、誰にでも、通知書を示された場合には、指定された資料を、理解できる形で提示させるか、そのために必要な関係資料(つまり暗号化キー)を開示させる権限を確立することを提案します。通知書を実施できることは、IOCA と PACE に含まれる既存の法的な権限に補助的な効力を与えます。すでに合法的に押収された、あるいは押収される資料だけに適応されることを意味します。