65. 新しい権限は、暗号化された通信やデータに合法的にアクセスすることはありません。守られなければ非合法になります。例えば、国務大臣発行の令状なしに、英国の公衆回線電気通信ネットワークで通信を傍受したら罪になります。不正に傍受された資料を解読する目的で暗号化キーにアクセスするために国務大臣の許可を得ることはできません。

66 新しい権限は、可能な限り技術的に中立です。例えば、暗号化キーとパスワードの境界線を引くのは難しくなってきています。実際、しばしば同じ目的で動作します。

67. 政府は、以下の場合に通知書を許可できるとしています。
・ 国務大臣が、令状のもとに傍受した通信の解読する特定の権限を与えている場合、または国家安全および諜報機関の場合に、諜報機関が法律上の機能を果たすために補助となる重要な役割を果たすと信じるに足るときに、そのための特定の権限を与えたとき。

(ページ30)
・ 保護されている資料を捜査、差し押さえ、提出するか、その他の方法で獲得する法律の条項によって、合法的な権限が存在する場合。

・ 保護されている資料を捜査、差し押さえ、またはその他の方法で獲得する裁判所によらない法律的権限(PACE の 18 節のもとで、逮捕後の立ち入りおよび捜査の権限)が存在する場合。これらの状況では、適切なレベルの特定の権限が必要です。(つまり、管理職以上のランクにある警察職員)

* 合法的に法の執行者が獲得した資料を、特定の目的で合法的に解読する裁判所の令状が得られている場合。

68 政府は、捜査機関がデジタル署名のためにのみ使われる暗号化キーにアクセスすることを可能にすることは提案していません。キーまたは資料の開示を要求する権限は公認または非公認の暗号化サービス提供者に適応されます。他の関連するキーを保持している者にも適応されます。しかしこれはプライベートの暗号化キーのコピーを保持する人には条件を規定しません。

69. 通知書は開示するべきキーまたは資料を特定します。、特別な場合には、指定された資料を判るような形(つまり書類の普通の文章)で提示するように要求するかあるいは関連する秘密のキーを開示するように命令するかどうか決定するのは権限を与えられた景観です。通知書はまた執行のもととなる特定の権限を指定します。将来問い合わせが有っても

監査がはっきり追跡できるような十分な情報を含みます。

70. 容疑者に暗号化キーを開示させる権限について、自分で罪を負わすのではないかという疑問があります。政府は自分で罪を負わすことに相当するとは考えません。提案されている権限は、容疑者に証拠を開示するように要求するのではなく、捜査当局にすでに確保されている証拠を分かる形にします。犯罪捜査の有効性を保つために、容疑者が強制される法律的な義務の例はいくらでもあります。(例えば、指紋の採取、DNA サンプル、自動車保険の証となる書面の証拠を提出するように要求されることなど)電子的な証拠を見える形にする権限無しには、犯罪者は犯罪行為を完全に罰せられないように隠してしまいます。政府はこれは公共の利益にかなうと考えていません。

71. 政府は合法的なアクセス条項がスコットランドや北アイルランドの異なる警察制度にどのように適応されるか検討しています。例えば、PACE の条項はスコットランドには適応されません。そこでは、捜査令状の法律は、法律条項でカバーされるある特定の形の捜査に関連する場合を除いて、一般的には自然法によってカバーされます。PACE の 20 節(コンピュータ化された情報の差し押さえについて警察を補助する)に規定される権限に相当するものはありません。

保障条項

72 法律は大規模な集合の解読キーには適応されません。

(ページ 31)
新しい権力は、暗号化された通信またはデータへのアクセスが既存の法律で与えられたときだけに有効になります。実際の運用はケースバイケースで行われます。

73. さらに、通知書が必要かつ適切な場面でのみ実行されるような法的な附則の保障条項があります。政府は新しい権限の実施を監督する Code of Practice に保障条項を附記しています。

74. 提案の法律は、通知書のもとに獲得した解読キーの安全とプライバシーを保護する強力な保障条項を含んでいます。傍受令状を発行する前に国務大臣が傍受した資料の取り扱い、開示、コピー、破棄について保障条項が整っていることを確認することを規定している IOCA の 6 節にあるものと同類です。通知書のもとに獲得した資料が、通知書が発行された目的のために保持する必要がなくなったら速やかに破棄されることが、法的な必要条

件となります。

監督と苦情

75. 政府は、国務大臣の権限の実施について、IOCAのもとで確立されたものと同じような方法で監督と苦情処理の機構を確立するつもりです。特に、これは国務大臣の大きな権限を独立して裁判所が監督することになることを意味します。政府は Commissioner and Tribunal を確立し、苦情を捜査する権限で、国務大臣の権力を監督して、必要とされれば、補償を行うことを考えています。

76. 例えば、裁判所が発行した捜査令状の遂行や提出命令で獲得したキーが関係する他の状況でも、既存の苦情の協定が適応されます。

罪と罰

77. 政府は新しい権限に関連した2つの新しい罪を制定するように提案します。

・ 通知書の内容に合理的な理由なしに従わない罪

・ 国務大臣が暗号化キーに合法的にアクセスするように許したことを人に「内報する」罪

78. 従わないことの罪を制定することは、可能な限り暗号化キーが開示されるために必要です。「内報する」罪は既存の法律(たとえば、麻薬取引)と矛盾せず、重大犯罪の極秘捜査の秘密を守るために考えられています。これらの罪に対する罰は、既存の法律の同様な罪と同程度となります。

79. 政府は暗号化キーへの合法的なアクセスの提案についての意見を歓迎します。

(ページ32)

パートナーシップ・アプローチ： 法執行機関と産業界のニーズの合致

キーエスクローと第三者によるキーリカバリー

80. 上記のプロポーザルは、適切に認証された書面による通知を送達することにより、通信データおよび保存データの暗号を解除することができるという仮定に基づいています。この通知が暗号化プロセスの管理下にある個人に送達された場合には、暗号化解除が可能となります。ただし、通信が傍受された場合には、法執行機関がその個人（たとえば、その通信を暗号化するドラッグ不正取引商人など）が気がつかないうちに、通信の暗号解除

を行えるようにする必要があります。

81. キーエスクローあるいは第三者によるキーリカバリーなどの暗号化技術は広く使用された場合、ユーザに利益を与えるものであるとともに、法執行機関の傍受の権限もそのまま確保されることになります。英国政府は、この使用と開発を促進させるため多数のオプションを検討しています。以前の管理機関は、絶対的なライセンシング管理形態案について話し合いました。この形態では、キーエスクローなしで暗号化サービスを提供することを違法とすることもできました。しかしながら、この管理形態ではキーエスクローなしでの暗号化の使用を禁止することもなく、英国における電子商取引の成長に多大な損害を与える原因となったかもしれませんでした。

82. 英国政府は、キーエスクローあるいは第三者によるキーリカバリー などの技術を促進することに真剣に取り組み続けています。しかしながら、電子商取引の市場は急速な発展をしており、業界はライセンシングスキームの一部としてキーエスクローあるいは第三者によるキーリカバリーの条件を強制すれば、英国における電子商取引の発展に不合理な規制となるであろうと大きな懸念を表明しています。つまり、ライセンシングスキームでは、TSP により提供される機密保持サービスにおいては、法執行によりキーへのアクセスを可能にしなければならないという条件を強制させることはないであろうことをベースに英国政府が話し合いを行っているからです。

パートナーシップアプローチ

83. 多数の暗号化に広い可用性を持たせることを法執行することで発生する重大な結果を、英国政府が過小評価している兆候があると見るべきではありません。政府は法的執行に利点があるものとして、この政策によるインパクトを細部まで監視していくことにしています。現時点で、暗号化することによるインパクトは非常に大きいものであっても、大きな犯罪と戦うような運用上へ重大なインパクトはありません。したがって、変化は非常に急速なものとなる可能性があります。

84. 英国政府は、世界最高の電子商取引環境を英国に作り上げるという目的を達成することに最善の努力をすることとし、さらに法的執行力の有効性を保持することで、全体として社会に責任を持つとしています。英国政府は、業界とパートナーシップを確立し、電子商取引の成長を促進しながら、法律の執行条件を進めていく方法を合わせて見極めようとしています。英国政府は法の執行と電子商取引の目的が、ライセンシングスキームあるいはその他の方法によりどのようにすれば達成されるかその方法についてのアイデアを受け付けています。

(ページ33)

法執行機関の必要性

85. このパートナーシップを促進させることを目的として、既存の法令による権限の効力をそのまま維持するためには、法執行機関に何が必要かを明確にしなければなりません。特に、利害関係に関わる通信について法執行機関に対しかなりの誤解があります。

86. 法執行機関が最も重要事項として要求することは、重大な犯罪と通信の相手先について知識を持っていないその他個人との間で通信の暗号解読が可能となる点です。法執行機関は通常、合法な会社組織間、あるいはその他の合法なクローズシステム内の暗号化通信にアクセスすることはありません。ただし、会社組織側にとっては、通信のプレーンテキストを回復する自社専用の機能を持つことには大きな理由（たとえば、不正手段の防止など）があります（トランジット時または休社時）。

87. e-コマース活動は、個人と会社組織と間で釣り合いがとられることになります。この活動に重大な犯罪活動が係わるような場合には、法執行機関は重大な犯罪と会社組織との間の通信にアクセスしなければならないことになります（たとえば、インターネットショッピング、航空券の販売など）。ただし、法執行機関は、必要に応じて合法な会社組織の協力を求めることには必要と考えています。

88. 傍受を行うことを目的として、考慮すべき重要な要因が他にも多数あります。暗号解読プロセスはタイムリー（できるだけ、リアルタイムに近いタイミングで）で行なわれること、かつ判らないように利用できること（すなわち、調査ターゲットがインターセプトを行われていることに気が付かないようにしなければならないこと）が要求されます。理想としては、法執行機関は1つの組織にアプローチすることでターゲットに送受信された通信をすべて読み取ることができるようにしたいとしています。プレーンテキストが個人や暗号化サービスのプロバイダーのどちらもその内容に気が付かない方法で提供された場合、暗号されたキーではなく、プレーンテキストとして受信することも可能になります。

89. 暗号化された保存データを観点として見た場合、法執行機関が必要とすることは、やや異なっています。たとえば、企業や個人の所有する暗号化された多種多様な保存データが、捜査や差し押さえで法令による権限下におかれることがあります。また、プレーンテキストが調査時に差し押さえられた特定の暗号化文書と本当に関連があるか、法執行機関は裁判で証明しなければなりません。このような場合、コンピュータを法廷証拠として最善に活用するため、法執行機関には保存データの暗号解読が必要となります。