欧州における暗号政策および暗号評価機関に関する調査報告

－電子署名法における暗号政策の調査報告書－

平成 13 年 3 月

情報処理振興事業協会

目次

はじめに・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・1

Ⅰ．調査の概要・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・2

Ⅱ．調査報告・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・9

第１章　欧州電子署名標準化イニシアチブ＜EESSI＞・・・・・・・・・・・・・・・9

１．EESSI の組織・・・・・・・・・・・・・・・・・・・・・・・・・・・・１０

２．EESSI の下でのガイダンス・・・・・・・・・・・・・・・・・・・・・・１７

３．ＥＵ加盟各国の産業界の EESSI に対する反応・・・・・・・・・・・・・・・・２５

第２章　イギリスの電子署名関連の法律および規則・・・・・・・・・・・・・・・・３０

１．電子署名の分野での政府の役割および機能・・・・・・・・・・・・・・・・３０

２．電子署名関連の最近の法律および規則・・・・・・・・・・・・・・・・・・・３１

３．電子署名関連の法律と規則に対する産業界の反応・・・・・・・・・・・・・・３４

第３章　イギリスの評価機関・・・・・・・・・・・・・・・・・・・・・・・・・３８

１．貿易経済省と tScheme・・・・・・・・・・・・・・・・・・・・・・・・・３８

２．通信電子セキュリティ・グループ（CESG）・・・・・・・・・・・・・・・・・・４４

第４章　フランスの電子署名関連の法律および規則・・・・・・・・・・・・・・・５６

１．電子署名に関する最近の法律および規則・・・・・・・・・・・・・・・・・・５６

２．電子署名関連の法律と規則に対する産業界の反応・・・・・・・・・・・・・・５７

第５章　フランスの評価機関・・・・・・・・・・・・・・・・・・・・・・・・・５８

１．国防総事務局・・・・・・・・・・・・・・・・・・・・・・・・・・・・・５８

２．Direction Centrate de la Securite des Systems d'Information（DCSSI）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・６０

第６章　ドイツの電子署名関連の法律および規則・・・・・・・・・・・・・・・・６４

１．電子署名関連の最近の法律および規則・・・・・・・・・・・・・・・・・・・６４

２．電子署名関連の法律と規則に対する産業界の反応・・・・・・・・・・・・・・６７

第７章　ドイツの評価機関・・・・・・・・・・・・・・・・・・・・・・・・・・・・６８
１．Bundesamt fur Sicherheit in der Infomatinstehnik（BSI）・・・・・６８
２．Bundesministerium fur Wirshaft und Technologie（BMWi）・・・・・７0
３．Bundesausfuhramt（BAFA）［連邦輸出局］・・・・・・・・・・・・・・・・７３

Ⅲ. 参考文書・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・７４

はじめに

インターネットの急速な普及により、新しい情報のインフラストラクチャが構築されつつあります。なかでも、電子商取引に関するインターネットの利用において、安全性の確保のためには、「電子署名」技術が重要であるとされています。欧州では、国際協調と調和に基づいた電子署名の実現に向けて、eEurope イニシアチブの一部として EESSI（European Electronic Signature Standardization Initiative）の指針のもと、各国において法的・技術的な整備が進められています。

また、暗号技術は電子化された情報の秘匿性及び非改竄性の確保の他、署名・認証を実現するための基盤技術です。暗号の標準化を巡る動きも急速に変化しつつあり、米国においては DES にかわる次世代の標準暗号として、“ Rijndael ”が昨年１０月に採用されました。一方、欧州では NESSIE(New European Schemes for Signature,Integrity, and Encryption) が暗号アルゴリズム評価プロジェクトとして発足し、評価結果が広く欧州産業界に受け入れられることを目的として、昨年１１月に第 1 回のワークショップを終了しています。

このような状況において、情報セキュリティの評価については ISO/IEC15408 に基づき評価技術の開発がすすめられていますが、暗号アルゴリズムについては規定外とされており、米国は独自の評価基準の下で暗号技術評価を実施しています。

本調査は、欧州（イギリス、フランス、ドイツ）で施行される電子署名法と各国の評価機関および施策についての情報収集を行い、米国に対応した欧州の動向を把握し、日本の電子政府の評価体制構築の参考となることを目的としています。

具体的には、Ⅰ部「調査の概要」で調査結果を概説し、Ⅱ部「調査結果」、第１章「欧州電子署名標準化イニシアチブ」では欧州における電子署名の枠組みと組織について、第２～３章「イギリスの電子署名関連の法律および規則」「イギリスの評価機関」ではイギリスにおける電子署名施策および関連評価機関について、第４～５章「フランスの電子署名関連の法律および規則」「フランスの評価機関」ではフランスにおける電子署名施策および関連評価機関について、第６～７章「ドイツの電子署名関連の法律および規則」「ドイツの評価機関」ではドイツにおける電子署名施策および関連評価機関についてそれぞれ詳述しています。

Ⅰ．調査の概要

第１章　欧州電子署名標準化イニシアチブ（ＥＥＳＳＩ）

欧州連合電子商取引プログラムにおける EESSI の位置：EESSI は、eEurope と呼ばれる大きな EU 政府／業界イニシアチブの一部であり、「電子商取引での欧州イニシアチブ」と呼ばれる 1997 年 4 月の欧州委員会の報告書から生まれた。この電子商取引の発展を促進するビジョンを概説している報告書を基にして、1999 年 12 月に正式に eEurope イニシアチブを開始した。

EESSI の法的基礎：EESSI の法的基礎は、電子商取引に関する 1999 EC 指令の実施を支援することである。この指令は電子署名の法的有効性に焦点を当てており、証明書、認証サービスプロバイダ、署名作成、認証デバイスのミニマム要件を識別している。

EESSI の目的：電子署名の標準の開発のために、EC 電子署名委員会は、政府／業界標準化プログラムとして、ICT 標準化委員会の下に EESSI を作るよう促した。

他の電子署名イニシアチブと EESSI の協力：EESSI は、他の標準化団体と業界コンソーシアムの標準化作業との重複を避け、グローバルなレベルで、または他の地域レベルにおける関連のイニシアチブと緊密に協力し、電子署名アプリケーションの国際的な相互運用性を保証するソリューションの開発に努める。

EESSI の管理：eEurope を担当している 3 つのヨーロッパ標準化機構（CEN, CENELEC, ETSI）は、ICT 標準委員会を設立した。ICT 標準化委員会の下で、EESSI 作業プログラムは、Bull の Claude Boulle 氏（フランス）が議長を務める運営グループの管理の下で実行されている。

EESSI の開発：1999 年 1 月に、ICT 標準化委員会は、プログラムの定義を開始するように「専門家チーム」に依頼した。チームは、民間部門と学会からのメンバーによって構成されている。iD2 Technoligies の Hans Nilsson 氏（スウェーデン）が「専門家チーム」を率いている。

EESSI 標準の開発：電子署名に関する EC の指令は、主として政府機関ではなくヨーロッパの標準化機構に向けられたものである。ICT 標準化委員会の枠組の中で、ESTI と CEN は、EESSI 標準の開発を担当している。EESSI は現在 9 つの標準の公表に向けて活動している。

各標準の目的および ETST と CEN の間での責任の分担一覧は次のとおり。

標準	タイトル	範囲
ETSI	CSP の政策	様々な信頼レベルで活動する CSP のミニマム基本要件を定義する
ETSI	電子署名フォーマット	通信アプリケーションでのデジタル署名の標準化のための要件を調査する
ETSI	適格証明書のプロファイル	X.509 証明書の適格証明書として使用に関する勧告を発行する
ETSI	タイムスタンプのプロトコルとフォーマットに関するプロファイル	オプションの数を減らし、相互運用性を高めるプロファイルを定義する
CEN/ISSS	安全な署名作成装置のセキュリティ要件	署名作成装置のセキュリティ要件を技術面で詳細に記述し、一貫した署名作成プロファイルを作成する
CEN/ISSS	署名作成のプロセスと環境	署名作成装置を越えた、関連するすべての実際的ニーズに焦点を当てる
CEN/ISSS	セキュリティ検証のプロセスと環境	検証に使用される製品やその管理を含め、署名検証プロセスのための相互関連要件を対象とした仕様を精緻化する
CEN/ISSS	信頼できるシステムや製品のセキュリティ要件	共通基準を基にした共通基準保護プロファイルを開発し、暗号化モジュールのセキュリティ要件と適切なセキュリティレベルを指定する
CEN/ISS	電子署名用製品やサービスの適合評価	電子署名製品やサービスに関して、適合評価や適合評価の全般的調整のための一般原則を定義する

ETSI の EESSI プロジェクトの管理：ETSI のセキュリティ部門（ETSI SEC）は、通信環境におけるセキュリティインフラとサービスを主に担当している ETSI 技術団体である。ETSI SEC は、通信と取引のレベルでの相互運用性の問題に関心が強く、電子署名インフラ（ESI）作業部会は EESSI 作業プログラムを担当している。

ETSI における標準開発の現状：ETSI は、4 つの EESSI 標準すべての草稿を完成している。電子署名フォーマットという草稿はすでに仕上がっている。その他の ETSI 成果物の最終承認と公表は、2002 年 5 月までに行われる予定である。

CEN の EESSI プロジェクトの管理：CEN の情報化社会標準化システム（CEN/ISSS）は、、電子署名ワークショップ（E-SIGN）を設立した。CEN の 5 つの EESSI 標準に関する技

術作業は、5 つの E-SIGN 作業部会内で実行されている。

CEN での標準開発の現状：各 CEN/ISSS プロジェクトチームは、標準草稿を開発した。2001 年 2 月 7 日の CEN/ISSS 会議において、以下の草稿が承認を受けるためにレビューされた。安全な署名作成装置、電子署名の認証手続き、適合評価のガイドライン。

EESSI に対する EU 加盟政府の支援：EU 加盟政府は、電子商取引のグローバルな性格が適用法の問題と、各国証明書の国際的な承認に関する手続き問題を提起しているというコンセンサスを表明した。電子商取引の発展には、電子署名の開発での地域協力が必要であり、EESSI は効果的なプログラムであるというコンセンサスが EU には広まっている。

電子署名標準に関する EU 産業界の懸念：EESSI の作成に関する EU 産業界の懸念は、次のものである。1）政府間調整の必要性、2）様々な技術を将来もオープンに、3）自主的的認定の作成、4）契約の自由の確保、5）法的枠組の確立、6）（政府開発の標準ではなく）民間によるオープン標準の開発を許す、7）国際的な調整作業。

EESSI に対する EU 産業界の支持：EU 産業界は、EESSI を強力に支援している。EC は、プログラムの開発において産業界のすべての懸念を検討した。産業界の支持は、広く知られているヨーロッパ標準化機構である ETSI と CEN の使用によって、さらに強化された。さらに、標準開発は、EU 産業界のメンバーからなる作業部会をベースにして行われている。これにより、標準は電子署名に関わる主な EU 企業から支持が得られた。その他の EU 企業は、ICT 標準化会議でへの業界団体の参加を通して EESSI に反映されている。EESSI に対する EU 産業界の支持は、多数のオープン会議によっても発展した。しかし、EESI はまだ標準化作業の大部分をまだ完成していないので、EESSI に対する EU 産業界の支持の最終レベルを今直ぐ判断するのは早計である。ほとんどの EESSI 標準はまだ草稿の段階であるからである。

第２章　イギリスの電子署名関連の法律および規則

電子署名に関する法：英国政府は、2000 年の電子通信法の下で電子署名に法的承認を与えた。この法の下では、紙にこだわる従来の法の障害は可能な限り取り除かれ電子署名に関する品質とサービスの最低標準を確保するために、自発的な「自己規制承認」スキームが確立されると思われる。法の検討過程で、英国政府は産業界や IT 産業から広く意見を募り、1.　政府は、義務としてのキーエスクローを法から削除、2.　法の執行権力は、この法案からホームオフィス調査権力法案に移行、の２点を取り入れた。

英国産業界の反応：電子通信法は、産業界と政府の間での数年間に渡る論議の結果であり、各層から広く支持されている法制度が生まれた。

第３章　イギリスの評価機関

貿易産業部：貿易産業部（DTI）は、2000 年の電子通信法を含む、電子署名に関する英国の法や規制の開発や実施を担当している。DTI が、直接電子セキュリティ製品やサービスを評価することはない。英国政府は、電子署名の品質とサービスの最低限の標準を確保するための「自己規制アプローチ」スキームを、産業界が開発するのを認めた。産業界主導の電子署名評価組織は、tScheme と呼ばれている。tScheme は、まだ企画の段階である。2000 年 11 月に、最初の４つの tScheme 承認プロファイルとガイドラインが tScheme 暫定委員会によって批准され、パイロットドキュメントプロジェクトとして公表された。どのパイロットプロジェクトも、2001 年 3 月前に完了することない。

通信電子セキュリティグループ（CESG）：CESG は、政府による暗号の正式使用のための、政府による国家技術局であり、一般的には情報セキュリティ（Infosec）のための技術局である。主な CESG 暗号評価プログラムは、CESG 支援製品スキームと英国 ITSEC（情報技術セキュリティ評価基準）認証スキームである。CESG 支援製品スキーム（CAPS）は、英国政府自身が使用する暗号製品に関わる企業のためのスキームである。メンバーは、適切な CESG が開発した暗号アルゴリズムを自社の製品に組み込み、それを CESG に提出して評価を受けることができる。承認されると、その製品は、英国政府御用達製品として公表される。

第４章　フランスの電子署名関連の法律および規則

電子署名に関する法：従来、フランスはヨーロッパで最も総合的な暗号化規制を実施してきたが、1998 年に非常に厳しい制限を課している政策を見直し始め、2000 年 2 月に、「証拠法と電子署名」という、電子署名に関する新しい法律を導入した。この法律は、フランスの証拠法を修正し、情報技術を検討し、電子ドキュメントや電子署名の法的効力を認めている。また、法は、電子署名に関する EC 指令をフランス法に組み込んでいる。

産業界の反応：1990 年代には暗号の使用に対するフランスの規制は世界で最も厳しいものであり、産業界は、規制がフランスの電子商取引の発展を妨げているとして、この規制を緩めるように政府に積極的に働き掛けてきた。この結果 1990 年代の後半までに、電子署名を含むすべての暗号の使用に関して新しい規制が実施されることになった。概して、フランス産業界は、電子署名に対する現在の政府の政策を支持している。これは、欧州電子署名標準化イニシアチブ（EESSI）における、フランスの先進的 IT 企業の１つである Bull の積極的な活動に示されているように、産業界の利害と一致している。

第５章　フランスの評価機関

国防総事務局（SGDN）：SGDN は、情報セキュリティを含む、広い範囲の国防問題についてフランス首相に助言と勧告を与え、情報システムのための省庁間委員会（CISSI）の長として活動し、機密情報や国防の秘密を守る委員会と共に政策を準備する使命を担っている。この役割を担って、SGDN は、情報システムセキュリティのためのフランス中央サービス（SCSSI）[1]とも呼ばれる、情報システムセキュリティの中央サービス（DCSSI）を管理している。

情報システムセキュリティの推進センター（DCSSI）：DCSSI は、フランス政府のセキュリティ活動と政策を担当し、主に公式の情報セキュリティ政策の開発と実装においてその他のフランス政府機関を支援している。DCSSI は、次の 3 部門から構成されている。規制部門はDCSSI の産業関係と国際関係を担当する。この部門は、情報セキュリティにおけるDCSSI の規制を作成・実行すると共に、認証サービスも提供する。運営分門は、通信や情報のセキュリティにおいてフランス政府の活動を支援する。科学技術部門は、情報技術、通信セキュリティ、暗号の分野で、技術支援を提供する。評価の分野では、DCSSI は、暗号製品を評価するために多数の認定プロファイル（または標準）を作成した。DCSSI 認証の通知は、認定報告書と共に、一般に公開される。DCSSI の暗号評価／認証プログラムは、欧州 ITSEC プログラムや共通基準と調整が図られている。D CSSI 暗号評価は、公認の情報技術セキュリティ評価センター（CESTI）によって実行される。

第６章　ドイツの電子署名関連の法律および規則

デジタル署名法：現在の電子署名に関する基本法は、1997 年のデジタル署名法である。デジタル署名法は、技術法でありデジタル署名の法的効力を扱っていない。この法律は、ドイツにおけるデジタル署名の使用のための安全なインフラの条件を提供している。2000 年９月デジタル署名法、民法、民事訴訟法が改正され、電子署名に対して、さらに高い法的効力が認められた。

ドイツ産業界の反応：一般に暗号に対する政府の強い規制には反対している。産業界は、BSI（連邦情報安全局）技術標準がベースの法は、デジタル署名普及の面で競争的な市場主導型にはならないという点で、従来のデジタル署名法の実施に懸念を抱いていた。そこで、デジタル署名規制の緩和を主張し、BSI 技術カタログの阻止、BSI 以外の認証機関を認めさせることに成功した。

[1] SCSSI と呼ばれていたが、最近 DCSSI として再組織された

第７章　ドイツの評価機関

情報技術安全連邦局（BSI）：BSI は、IT と暗号分野の政府機関であり、主に政府が IT システムを維持するのを支援しており、たとえば、ドイツ CERT プログラムを支援している。また、BSI は、次の２つの分野で商用暗号プロジェクトの評価と認証を提供している。（通信および郵便の規制機関を支援して）電子署名とセキュリティ製品。英国やフランスと同様に、ドイツは、ITSEC と共通基準プログラムに参加している。BSI は、双務または多角協定に基づいて他の認証機関の ITSEC や CC 証明書を認めている。ITSEC と共通基準に入るプロファイルを認めている他に、BSI は応用と解釈に関する注（AIS）も発行している。BSI 自身が認証を実施している。しかし、製品の技術的評価は、一般に BSI が認可し許可している評価機関（ITSEF－IT セキュリティ評価機関）が行っている。BSI 認証の通知は、認証報告書と共に公表される。

経済技術省（BMWi）：BMWi は、主に、情報技術の分野での BMWi の活動を担当する通信郵便の規制機関を始めとする、いくつかの下部機関を持っている。規制機関は、デジタル署名の認証と承認を規制しており、この分野は、BSI によって支援されている。規制機関は「国家ルート認証機関」とも呼ばれて、認証におけるトップレベルの機関である。

連邦輸出局（BAFA）：BAFA は、経済技術省（BMWi）の機関であり、ドイツの主な輸出規制許可機関として、ドイツ暗号製品の輸出の審査を担当している。しかし、BAFA は、ドイツ政府やドイツ民間部門で使われる、暗号製品を技術的標準に従って評価したり認証したりすることは行っていない。

なお、暗号の技術評価に関して特記すると、イギリス、フランス、ドイツのそれぞれの国では、政府自身が使用する暗号アルゴリズムの開発を行い、技術評価をしていると推定されるが、公開はしていない。（ただし、ドイツはデジタル署名法に基づく安全な暗号アルゴリズムの評価を行い、公開している。推奨暗号アルゴリズムの要件定義をしており、FIPS 140 を参照している。）一方、市場に出回る暗号製品やサービスプロバイダのセキュリティ評価は行っており、公開もされている。

欧州各国で独自に行われている暗号技術評価の実態は推定の域を出ないが、欧州委員会の「情報化社会技術」の一環として活動している NESSIE（New European Schemes for Signatures, Integrity, and Encryption）プロジェクトは公開されている。NESSIE は米国の次期暗号標準 AES（Advanced Encryption Standard）が選定される前の 2000 年５月に「AES 最終候補に関する NESSIE 計画のコメント」と題した分析結果を米国政府に提出したりもしている。また NESSIE 自身の目的が、今後の暗号規格およびプロトコル

の基礎として使用可能な一連の強力な暗号基本方式を開発することにあり、現在ブロック暗号、同期式ストリーム暗号、非対称暗号等のアルゴリズムを全世界から募集し、2000 年 11 月には応募者を集めて作業部会を開催した。2002 年 12 月までには最終選定を終える予定である。NESSIE が一連の基本案を組み合わせる作業を完了した場合、欧州委員会は NESSIE の成果を幅広く普及させて、NESSIE 産業委員会、第５次枠組み計画および様々な標準化組織などを含めた適切な公開討論会を通じて、規格およびプロトコルに関するコンセンサスを得ることを計画している。

また、評価方法（安全性評価および性能評価の両方）を確立し、候補となる基本案の評価を支援するソフトウェア・ツール群を開発して、暗号分野の標準化に影響を及ぼすものと予測されている。NESSIE はヨーロッパでの暗号標準化に関して大きな影響力を持っており、また今後長期間に渡り、世界的にもある程度の影響力を有すると思われる。

Ⅱ．調査結果（*）

第１章　欧州電子署名標準化イニシアチブ（ＥＥＳＳＩ）

欧州電子署名標準化イニシアチブ（EESSI）は、1999 年 12 月 13 日の電子署名に対する EC 指令を支援するため、欧州情報通信技術（ICT）標準化会議の後援を得て推進される標準化プログラムである。ICT 標準化会議は、欧州委員会（EC）と協力し、欧州通信標準化機構（ETSI）と欧州標準化委員会（CEN）から、プロジェクトに対し技術的支援を受けている。EESSI が開発した電子署名製品の標準は EC を通じて公表されることとなる。欧州連合（EU）加盟各国の法は、製品がこの標準に準拠しているとき、イニシアチブで設定されている要件に準拠しているものと想定する。

＜標準開発における EESSI の 3 大原則＞

・電子署名という広い分野に関わるすべての関係者の積極的関与
・イニシアチブが使っている、または採用しているメカニズムの開放性と透明性
・作業の重複を回避し、グローバルで国際的に認められたソリューションの奨励

＜標準化の対象分野＞

・証明書サービスプロバイダに対する政策
・信頼できるシステムと製品のためのセキュリティ要件
・安全な署名作成装置のセキュリティ要件
・電子署名フォーマット
・署名作成のプロセスと環境
・セキュリティ検証のプロセスと環境
・適格証明書のプロファイル
・タイムスタンプのプロトコルおよびフォーマットのプロファイル

いくつかの EESSI 標準はすでに公表されている。EESSI は、2001 年／2002 年までに残りの標準開発作業を終了する予定である。

本章では EESSI に関する次の項目を報告する。

１．EESSI の組織
２．EESSI の下でのガイダンス
３．EU 加盟各国や産業界の EESSI に対する反応

＊報告の中の（参考文書××）そのものは掲載していません。参考文書一覧はⅢを参照してください。

１．EESSI の組織

EESSI プログラムは、EC の電子署名イニシアチブがまだ草稿の段階であった 1998 年に始まり、多数の標準化機構と共同して、欧州連合内での電子署名の使用を促進する作業プログラムを開発している。

（1） eEurope イニシアチブ

EESSI は、eEurope と呼ばれる大きな EU 政府／産業界イニシアチブの一部である。eEurope イニシアチブは、「電子商取引における欧州イニシアチブ」と呼ばれる 1997 年 4 月の EC 報告書（参考文書A1）から始まった。この報告書は、欧州連合で電子商取引の発展を促進するための EC ビジョンを概説している。この報告書を基にして、欧州委員会は、1997 年に eEurope イニシアチブの開発を開始し、1999 年 12 月に正式にプログラムを立ち上げた。

eEurope イニシアチブは、欧州経済を近代化し電子ビジネスを促進するための主な EC プログラムである。

＜eEurope イニシアチブの目的＞

・すべての市民、家庭、学校、企業、政府をオンラインで結ぶ。

・デジタル技術に強い活気のある欧州を作り出す。

・社会的に包括的な情報化社会を実現する。

eEurope イニシアチブの標準開発において、EC は以下の 3 つの欧州標準化機構（ESO）から支援を得ている。

・欧州通信標準化機構（ETSI）

・欧州標準化委員会（CEN）

・欧州電子技術標準化委員会（CENELEC）

これら 3 つの組織は、eEurope イニシアチブを支える IT 標準化の共通アクションプランを開発した。アクションプランの目標の 1 つは、欧州会議と欧州委員会のガイドラインを基にして、EESSI を適切に管理することである。

(2) 電子署名に関する欧州会議のガイドライン

全世界で、電子署名に関して複数の標準化イニシアチブが存在している。これらのイニシアチブは、国家、地域、国際レベルで政府と産業界の組織による共同作業を含んでいる。この作業のいくつかの例を挙げるならば、国際商工会議所後援のプログラム、インターネット法政策フォーラム、インターネットエンジニアリングタスクフォース、ワールドワイドウェブコンソーシアム、米国弁護士会などがある。

しかし、電子署名の「欧州標準」を普及させるためには、欧州連合は「連合規模の」標準化プログラムを必要としており、他の標準化作業は、デジタル署名の EU の総合的な法

的要件に応えるには、不十分であると考えている。電子商取引を加速させるために、電子署名の標準化を eEurope イニシアチブのキーコンポーネントとしている。

しかし、欧州会議は、既存の標準化機構の作業を無視するのではなく、むしろできる限り標準化を基にした電子署名の一貫し統一した法的枠組や、ヨーロッパばかりでなく、国際レベルでも法的に承認された署名を提供するのに使うことができる自主的な協定を作成することに努めてきた。

＊（注）：欧州連合の組織は、欧州委員会（権力機関）、ヨーロッパ会議、欧州議会、裁判所から構成されている。ヨーロッパ会議は、主に EU 加盟各国政府の首脳がほぼ定期的に集まる会議として存在している。この「サミット」は、1970 年代の前半に定期的に開催され、1974 年のパリサミットでヨーロッパ会議と命名される前に、1960 年代の前半にすでに実際上設立されていた。ヨーロッパ会議の主な役割は、欧州連合に関する条約の一般規定条項４で次のように述べられている。「ヨーロッパ会議は、連合に対して発展の促進者となり、そのための一般的な政治原則を定義しなければならない。」

（3）電子署名に関する EC 報告書と提案

欧州委員会（EC）は、1997 年 10 月に「電子通信での安全と信頼を確保する－デジタル署名と暗号化の欧州枠組に向けて」という第 1 草稿（参考文書A3）を提出した。1997 年 12 月に、欧州会議は、委員会に対して、できるだけ速やかに特にデジタル署名に関するイニシアチブに対する提案を提出するように求めた。1998 年 12 月に、委員会は、「域内市場での電子商取引の法的側面に関する提案」（参考文書A4）を提出した。

（4）電子署名に関する 1999 年指令

欧州委員会がその提案を提出してから 1 年後、欧州議会は、1999 年 12 月 13 日に電子署名の EU 法的枠組を提供するという EC の指令（参考文書A5）を承認した。この指令の意図は、認証のすべての適用分野に取り組むのではなく、電子署名の法的な有効性に絞り込むというものである。

指令は、適格証明書、認証サービスプロバイダ、署名作成のプロセスと環境のミニマムな要件を次のように定めている。

指令の付録１（Annex Ⅰ：Requirements for qualiied certificates、参考文書A5 以下 Annex Ⅱ～Ⅳについても同じ参考文書A5）は、**適格証明書の要件**を記載している。適格証明書は、次のものを含んでいなければならない。

（a）証明書が適格証明書として発行されたことを明記

（b）認証サービスプロバイダの証明とそのプロバイダが設立されている国

（c）署名者の名前または匿名、それぞれしかるべく識別されていること

（d）証明書の当初の目的に依存して、適切な場合、署名者の特定の属性を含めるという規定
（e）署名者のコントロールの下での署名／作成データに対応する署名／検証データ
（f）証明書の有効期間の開始日と終了日
（g）証明書の識別コード
（h）証明書を発行する認証サービスプロバイダの高度な電子署名
（i）該当する場合、証明書の使用範囲の制限
（j）該当する場合、証明書が使われる取引価値の制限

指令の付録 2（AnnexⅡ：Requirements for certification-service-providers issuing qualified certificates）**は、適格証明書を発行する認証サービスプロバイダの要件を記載している。認証サービスプロバイダは次のことを実行しなければならない。**

（a）認証サービスを提供するのに必要な信頼性を証明する
（b）迅速で安全なディレクトリと安全で迅速な取り消しサービスのオペレーションを保証する
（c）証明書が発行された、あるいは取り消された正確な日時を提供できる
（d）国内法に従った適切な手段を使って、適格証明書の発行先となる者の身元と、適切な場合には、特定の属性を検証する
（e）提供するサービスに必要な専門知識、経験、資格、特に管理者レベルの場合には、能力、そして電子署名技術の経験と適切なセキュリティ手続きの詳細知識を持っている者を雇う。また、すでに承認された標準に適合した管理手続きを適用しなければならない
（f）改竄を防ぐことができる信頼できるシステムや製品を使い、使用している暗号の技術的セキュリティを保証する
（g）証明書の改竄に対処し、認証サービスプロバイダが署名作成日を作成する場合には、そのようなデータの作成中の秘密を保持する
（h）適切な保険の利用等により、特に損害に対する責任を引き受けるために、指令で定められている要件に従い、運営に十分な資金を保持する
（i）一定の期間、特に訴訟のために証明書の証拠を提出する場合に備えて、適格証明書に関するすべての情報を記録しておく。このような記録を自動的に行うこともできる
（j）認証サービスプロバイダが鍵管理サービスを提供している者の署名作成データを保存あるいはコピーしない
（k）自分の電子署名をサポートする証明書を求める人と契約関係に入る前に、その者に対して、使用の制限、自主的認定スキームの存在、トラブルや係争解決のための手続きを含め、証明書の使用に関わるすべての条件を恒久的な通信手段によって知ら

せる。電子的に伝送してもよい。この情報は書面で用意し、分かりやすい言語で書かれていなければならない。この情報の関連部分も、求めに応じ、証明書を信頼している第三者に提供しなければならない

(l) 信頼できるシステムを使用して、証明可能な形式で証明書を保存することにより下記項目を実現する。

－有資格人だけが記入あるいは修正できる

－情報の真性をチェックできる

－証明書の所有者の同意が得られた場合にのみ、証明書を誰でも検索できるようにする

－セキュリティ要件を損なういかなる技術的な変更もオペレータに明白である

付録 3（AnnexⅢ：Requirements for secure signature-creation devices）は、**安全な署名作成装置の要件**を記載している。

1. 安全な署名作成装置は、適切な技術的手段および手続きによって、少なくとも次の条件を満していなければならない
   （a）署名作成に使われる署名作成データは実際に 1 回のみ作成でき、その秘密が適切に確保される
   （b）署名作成に使われる署名作成データは、合理的な確実性をもって、導出することができず、現在利用可能な技術を使った署名の改竄が不可能である
   （c）署名作成に使われる署名作成データは、他の者による使用に対して正当な署名人により適切に保護される
2. 安全な署名作成装置は、署名されるデータを変更してはならず、またそのようなデータが署名に先立ち署名人に必ず提示されなければならない。

付録 4（AnnexⅣ：Requirements for secure signature verification）は、**安全な署名検証のための勧告**を記載している。署名検証プロセスでは、合理的な確実性をもって、次のことを保証しなければならない。

（a）署名の認証に使われるデータは、確認のために表示されるデータに対応していなければならない

（b）署名者は、高い信頼性をもって検証され、その認証の結果が正しく表示されなければならない

（c）認証者は、必要に応じ、署名入りのデータの内容を高い信頼性をもって設定できる

（d）署名認証時に必要な証明書の真性と有効性が高い信頼性をもって認証される

（e）認証の結果と署名者の身元が正しく表示される

（f）匿名が使われていることが明確に示される

（g）いかなるセキュリティ関連の変更も削除できる

（5）EESSI の管理

ICT 標準化会議の下で、EESSI 作業プログラムは、Bull の Claude Boulle 氏（フランス）を議長とする運営グループの管理下で実行されている。Boulle 氏は、ETSI から 1 人、CEN から 2 人の代表を含む事務局（3 人）からの支援を得ている。ETSI と CEN が、EESSI のほとんどの技術的作業を行っている。運営グループには、次の標準化機構の代表も加わっている。

- 国際標準化機構（ISO）
- Euroscom
- 欧州電子ビジネスフォーラム（EEMA/ECAF）
- 欧州バンキング標準化委員会（ECBS）
- 欧州計画会議（ECP）

また、他の公的機関、市場参加者、EC スタッフのメンバーも参加している。運営委員会のメンバーは次のとおりである（2000 年末現在）。

EESSI 運営グループのメンバー		
機能	名前	企業／組織
a. 正式メンバー		
議長	Claude Boulle	Bull
	Yves Chauvel	ETSI
	John Ketchell	CEN
	Georgia Skouma	CEN
b. EESSI 補助エンティティ		
ETSI	Gyorgy Endersz	Telia
CEN	H. Nilsson	ID2 Technologies
c. 標準化機構		
ISO	Walter Fumy	Siemens AG
Eurescom	Olivier Delos	Belgacom
EEMA/ECAF	Frank Jorissen	Utimaco Safeware
ECBS	Leon Peeters	ECBS
ECP	Rene van den Assem	ECP
d. 公的機関と消費者代表者		
	Tapio Aaltonen	Population
	Roberto Benzi	Autorita per l'informatica nella Pubblica Administrazione

	Leonidas Kanellos	European Association for the Co-ordination of Consumer Representation in Standardization（ANEC）
	Klaus Keus	British Standards Institute
	Laurent Perdiolat	Ministere de l'Economie, des Finances et de l'Industrie
e. マーケットプレイヤ代表者		
	Ignacio Alamillo	Agencia Certifications Electronica
	Andreas Mitrakas	Globalsign
	R. Temple	British Telecommunications
f. 欧州委員会		
	Anne Lehouck	EC
	Theodor Schlickmann	EC
	Andrea Servida	EC
	Joep van der Veer	EC

（6）ETSI と CEN での技術作業を調整

電子署名に関する EC 指令は、主として政府機関ではなくヨーロッパの標準化機構に向けられたものであり、EC 指令によって述べられている最低法的枠組に準拠した、実行枠組を設定することである。こうして EC は、ビジネスニーズに応え、オープン電子商取引環境の発展のサポートにおいて電子署名の法的承認を最大限に活用しようとしている。

ICT 標準化会議の枠組内で、ESTI と CEN は必要に応じて他の組織と協力して、EC の電子署名指令に述べられているように、基本的な法的枠組の支持する標準化活動に対するニーズの分析を担当している。これら ETSI や CEN の技術会議は通常協力を促進するために同じ場所で開かれる。ESTI であれ CEN であれ、通常、作業は、すべての関係者に対して開かれている。

・欧州通信標準化機構

欧州通信標準化機構（ETSI）は、CEN や CENELEC とともに 3 つの公認標準化機構（ESO）の 1 つである。ETSI は、南部フランスの研究パークであるソフィア・アンティポリスに本部を置く非営利団体である。欧州全体で使われる通信標準の作成が役割である。ETSI には、ヨーロッパ内外の 52 ヶ国のメンバー約 8000 人がいる。各メンバーは、政府、ネットワーク業者、メーカ、サービスプロバイダ、研究機関、ユーザを代表している。ETSI は「オープンな」組織（参考文書Ａ７）であり、欧州通信標準の促進に関心を持つ組織ならば、ETSI でその利害を代表し、直接標準作成過程に影響を与える権利を持っている。

EESSI の作業の他に、ETSI は、情報通信技術標準化協会（ICTSB)、グローバル標準共同体（GSC)、グローバル無線標準化機構（RAST）のような、多数の他のイニシアチブに参加し、またこれらのイニシアチブを支援している。

ETSI のセキュリティ部門（ETSI SEC）

ETSI のセキュリティ部門（ETSI SEC）は、EESSI に関する ETST の作業を担当している。ETSI SEC は、ETSI 内の技術団体であり、主に通信環境のセキュリティインフラとサービスを担当している。ETSI SEC は、信頼関係の面ばかりでなく、通信や取引のレベルでの相互運用性の問題に特別の関心を払っており ETSI ESI WG が EESSI 作業プログラム関連を担当している。

・欧州標準化委員会

欧州標準化委員会（CEN）は全世界の組織やヨーロッパにおけるそのパートナと共同して、ヨーロッパの自主的な技術的調和の促進を使命としている。CEN は、CENELEC が扱っている電気技術や ETSI が扱っている通信を除く、すべての経済活動の分野における欧州標準を企画、草案作成、採択する唯一の公認欧州組織である。CEN は、ISO（国際標準化機構）と技術協力のための協定（ウィーン協定）を結んでいる。

CEN は、ヨーロッパの様々な利害を代表しているメンバーから構成されている。

情報化社会標準化システム（CEN/ISSS）

情報化社会標準化システム（CEN/ISSS）は、下記の EESSI 作業プログラムを担当している。

・署名作成および認証製品の品質および機能標準

・認証サービスプロバイダ（CSP）の品質および機能標準

CEN/ISSS は、その作業において、従来の CEN 技術委員会の他に、ワークショップ（すなわち、専門プロジェクトの作業部会）メカニズムを使っている。CEN/ISSS ワークショップは、すべての関係者に開かれており、全員一致の原則により運営され、仕様、暫定標準、ガイドラインなどを作成している。

EESSI 作業プログラムの一部を実行するために、CEN/ISSS は、電子署名ワークショップ（E-SIGN）を創設し 1999 年 12 月にその作業を開始した。

19iD2 Technologies のコンサルタントであり、EESSI フェーズ 1 の専門家チームのリーダーである Hans Nilsson 氏がワークショップの議長に指名された。ドイツ標準化機構（DIN）に E-SIGN 事務局の運営が任された。E-SIGN プロジェクトチームは、5 つの作業分野から構成される。その活動は、2-（5）CEN／ISS の成果物で説明する。

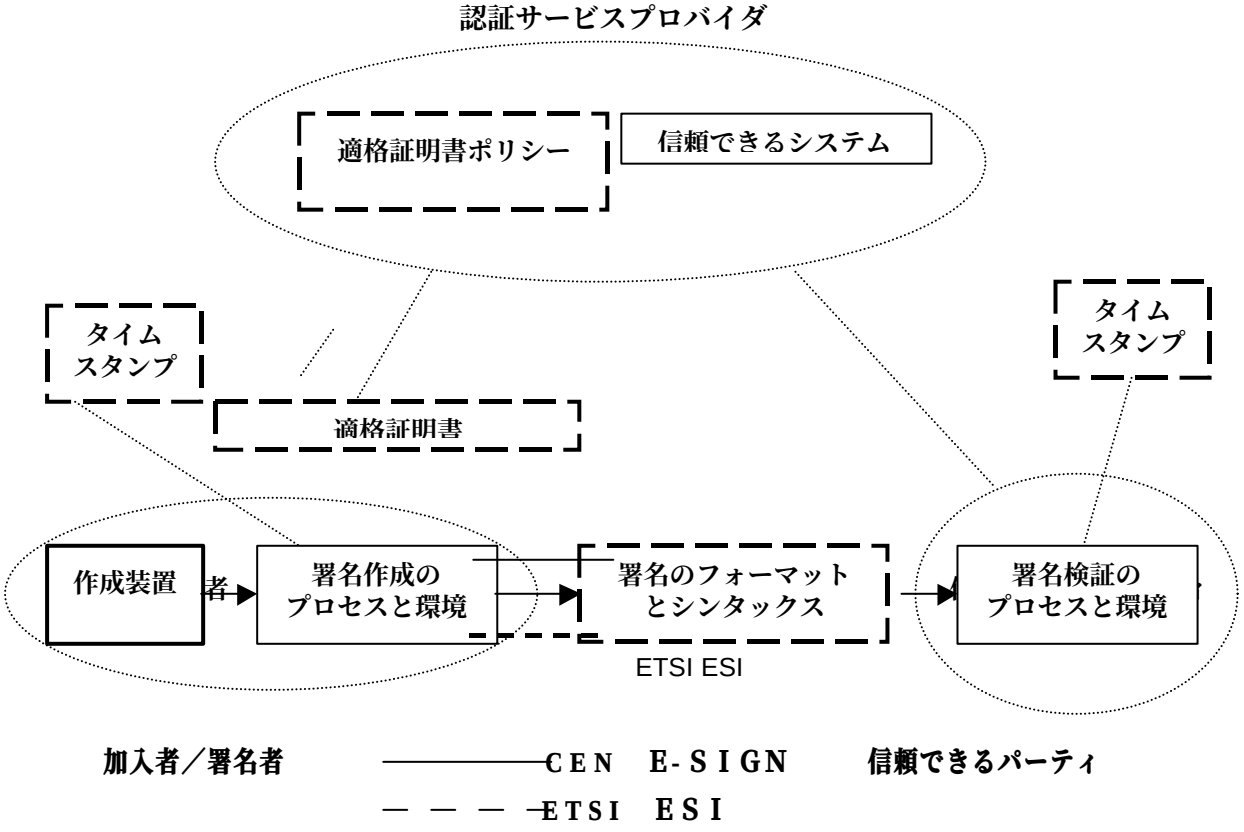
２．EESSI の下でのガイダンス

電子署名に関する EC 指令は、電子署名を使うセキュリティインフラや認証サービスの調和のための、ヨーロッパにおける包括的な法的枠組を提供している。しかし、加盟各国の法においてその法的規定を完全に実施するには、EESSI からの適切な技術的支援が必要である。

EESSI の枠組内で、CEN/ISSS と ETSI/SEC は、EC 指令の完全な実施のために必要な標準化の作成を任されている。CEN/ISSS と ETSI/SEC は、多数の会議を持ち、いくつかの報告書を作成し、EESSI の下で標準化を発表し始めている。

（1）EESSI の成果物

2000 年 5 月のセミナーから、EESSI 運営グループは、EESSI の実際の成果物を説明している EESSI 文書（参考文書Ａ１３）を作成した。文書は適用標準の開発における電子署名アーキテクチャに対する EESSI のビジョンと CEN と ETSI の特定の責任を示している。また、以下では各 EESSI 成果物を説明している。



EESSI 標準の枠組と電子署名の種類：本作業の目的は、EESSI プログラムの一般的アーキテクチャを説明している参照枠組を作成し保守することである。また、CEN/ISSS と ETSI SEC からの様々な成果物を使って、いろいろな種類の電子署名の様々な要件にどの

ように対応するのかにも取り組んでいる。

認証サービスプロバイダ（CSP）に対するポリシー：この作業項目は、ヨーロッパで法的承認を得る電子署名をサポートするために、証明書を発行する CSP の運営や管理のための機能および品質標準を対象としている。成果物は、CSP 特定の信頼レベルの仕様を提供し、ETSI 標準のフォーマットを持っている標準要件仕様である。

信頼できるシステムや製品のセキュリティ要件：この作業項目は、（国際標準 ISO 15408 として開発されている）共通基準を基にして共通基準保護プロファイルを作成し、暗号化モジュールのセキュリティ要件と適切なセキュリティレベルを指定することを目的としている。この分野で開発される成果物は、共通基準保護プロファイルと使用される暗号化モジュールの要件とのセットである。成果物は、「電子署名用の適格証明書の発行において使用される信頼できるシステムのセキュリティ要件」という暫定タイトルを持つ、CEN/ISSS ワークショップ協定（CWA）形式のプレ標準である。

安全な署名作成装置のセキュリティ要件：この作業項目は、署名作成装置のセキュリティ要件を技術的に詳細に記述し、一貫した署名作成プロファイルを作成することを目的としている。これは、保護プロファイルの形式を取る標準の開発によって行われる。情報技術セキュリティ評価（ISO 15408）用の共通基準を、保護プロファイルのために基本参考として使う。成果物は、「安全な署名作成装置のセキュリティ要件」という暫定タイトルを持つ、CEN/ISSS ワークショップ協定（CWA）の形のプレ標準である。このプレ標準は、安全な署名作成装置の共通基準保護プロファイルを含む。

電子署名フォーマット：この作業は、複数の署名や役割のサポートを含め、電子署名の標準フォーマットを確定し、審判者などが共通ツールを使って、その初期使用後の長い期間電子署名の有効性を検証できるようにすることを目的としている。標準の基本機能は、信頼できるタイムスタンプや取り消し日のような確認情報を電子署名の一部として含む。署名ポリシーのコンセプトは、電子署名の妥当性確認のために共通の基礎を確立するために、やはり重要なものであると確認されている。この作業分野の最初の結果である ETSI 標準「電子署名フォーマット」は、2000 年 3 月の ETSI メンバー投票によって承認されている。現在の活動の主な目的は、この作業を押し進め、さらにヨーロッパ基準へと進むばかりでなく、IETF や W3C を含む他の国際的活動との調和を図ることである。この作業は、外部活動との調和に必要なインターネット RFC、ETSI 標準、その他の改訂の作成を含む。

署名作成のプロセスと環境：この作業項目は、署名作成装置を越え、署名作成のプロセスと環境に関係している、すべての実際のニーズに焦点を合わせることを目的としている。

この要件は、電子署名の作成や署名環境用の高度なセキュリティを持つ製品の機能および品質要件の仕様として取り組まれる。この分野の仕様は、ガイドラインのセットに含まれ、その採用は製品サプライヤやユーザの意思に任される。これは、技術的に中立であるように配慮しているが、スマートカードやパーソナルコンピュータのような特定の技術のためのガイドラインを提供する。成果物は、「電子署名作成のためのユーザインタフェースと動作環境」という暫定タイトルを持つ、ガイドラインセットの形のプレ標準であり、CEN/ISSS ワークショップ協定（CWA）内で作成される。

署名確認のプロセスと環境：この作業項目は、確認や確認の管理に使われる製品を含め、署名確認のプロセス要件および関連要件を扱っている仕様を精緻化することを目的としている。さらに、この仕様のガイドラインセットは、特に署名確認環境が自動化署名確認コンピュータプログラムだけから構成されている署名確認環境に取り組む。成果物は、「電子署名検証の手続き」という暫定タイトルを持つ、ガイドラインセット形式のプレ標準であり、CEN/ISSS ワークショップ協定（CWA）内で作成される。

適格証明書のプロファイル：証明書の内容やフォーマットの標準化は、電子署名の確認に関して相互運用性を確保するために重要である。「適格証明書」というトピックで、作業がすでに IETF で開始されている。IETF 作業は、指令の付録 I に関係する声明の相互運用可能な包含と、国家アイデンティティスキームのようなその他の地域要件を実施するために必要な、地域プロファイリングを可能にする国際プロファイリングを提供する。そうした包含の例としては、証明書を使うことができる取引価値の制限がある。この作業項目は、不断に発展している IETF RFC を基にした欧州プロファイルを指定することを目的としている。標準は、指令の付属文書 I（参考文書A5）に従った適格証明書ばかりでなく、X.509 証明書の相互運用的使用の勧告を提供する。成果物は、IETF RFC を基にした適格証明書の欧州プロファイル向け ETSI 標準である。

RFC を基にしたタイムスタンプのプロトコルとフォーマットのプロファイル：安全なドキュメント交換一般のコンテキスト、またそうしたトランザクションの長期的な検証のために、タイムスタンプの意義について認識が高まっている。標準フォーマットとプロトコルは、タイムスタンプの相互使用にも対応している。作業はすでに「適格証明書」というトピックで IETF において開始されており、今年には RFC の状態に達すると考えられている。必要なデータ構造は、IETF RFC で定義されるが、オプションの数を減らし、相互運用性を高めるために、いくつかのプロファイルの定義が必要になるかもしれない。成果物は、IETF RFC を基にした、タイムスタンプのプロトコルとフォーマットのための ETSI 標準プロファイルである。

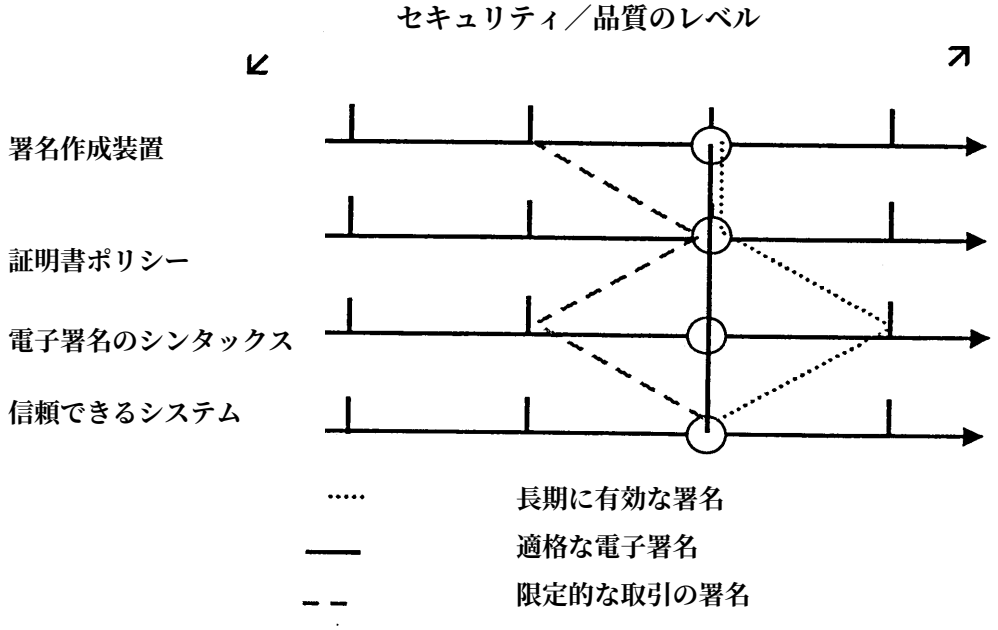
電子署名用製品やサービスの適合評価：適合評価は、CSP のサービスの規定やその監視、署名作成確認装置の使用や信頼できるシステムおよびメカニズムの前提条件である。言い換えれば、適合評価は、その評価と認証の両方から見て、すべての EESSI 成果物に必要である。成果物は、「電子署名製品とサービスの適合評価のためのガイドライン」という暫定タイトルを持つ CEN/ISSS ワークショップ協定（CWA）形式の、ガイドラインセットである。

（2）EESSI 標準の枠組と電子署名の種類

2000 年 9 月に、EESSI は、「電子署名標準化：国際レベル」というセミナーをバルセロナで開催した。

この会議から、EESSI 運営委員会は、電子署名の標準化と種類の枠組に関する最新報告書を発表している。各標準化が複数の要件を対象にしているので、EESSI が標準セットと、各標準化、「プロファイル」の使用を識別し、特定のビジネスニーズに対応することが必要である。そうした標準セットとその使い方は電子署名の種類を定義している。（参考文書 A15）

EESSI 標準の枠組と電子署名の種類



（3）EESSI 作業計画

先に示したように、EESSI の特定の成果物の開発は CEN と ETSI に分けられている。CEN は、5 つの EESSI 成果物を担当し、ETSI は 4 つの EESSI 成果物を担当している。

標準	タイトル	範囲
ETSI 標準	認証サービスプロバイダ（CSP）に対する政策	様々な信頼レベルで運営されている CSP の基本最低要件を定義する
ETSI 標準	電子署名フォーマット	通信アプリケーションでのデジタル署名の標準化のための要件を調査する
ETSI 標準	RFC を基にした適格証明書のプロファイル	EU 指令の付録 1 に従い、X.509 証明書を適格証明書として使用するよう勧告する
ETSI 標準	RFC を基にしたタイムスタンプのプロトコルとフォーマットのプロファイル	RFC YYYY で定義されているデータ構造を基にして、オプションの数を減らし、相互運用性を高めるために、RFC YYYY にプロファイルを定義する
CEN/ISSS ワークショップ協定	安全な署名作成装置のセキュリティ要件	署名作成装置のセキュリティ要件を技術レベルで詳細に記述し、一貫した署名作成プロファイルを作成する
CEN/ISSS ワークショップ協定	署名作成のプロセスと環境	署名作成装置から外れる、実際的ニーズのすべてに焦点を当てる
CEN/ISSS ワークショップ	セキュリティ確認のプロセスと環境	確認や管理に使われる製品を含めて、署名確認プロセス向けの相互に関連した要件を対象とする仕様を精緻化する
CEN/ISSS ワークショップ協定	信頼できるシステムや製品のセキュリティ要件	共通基準を基にした共通基準保護プロファイルを開発し、暗号化モジュールのセキュリティ要件と適切なセキュリティレベルを指定する
CEN/ISSS ワークショップ協定	電子署名用製品やサービスの適合評価	電子署名製品とサービスに関して、適合評価と適合評価のプロセスの全般的調整のための一般原則を定義する

（4）ETSI SEC からの成果物

成果物：ETSI は、4 つの EESSI 標準のすべての草稿を完成している。1 つの草稿（電子署名フォーマット）は最終段階にある。他の ETSI 成果物の最終承認と発表は、2002 年 5 月が予定されている。ETSI 作業成果の現状は次のとおりである。

タイトル	初稿日付および参考文書	完成予定日
適格証明書を発行する認証機関のポリシー要件	２０００年１２月６日 A18	２００２年５月
適格証明書プロファイル	２０００年９月２１日 A19	２００２年５月
タイムスタンプ プロファイル	２０００年１１月２１日 A20	２００２年５月
電子署名フォーマット	２０００年１１月２１日 A21	２００２年５月

（5）CEN/ISSS からの成果物

各 CEN/ISSS プロジェクトチームは、その担当エリアの標準化草稿を作成した。2001 年 2 月 5 日現在、最新の E-SIGN 草稿成果物は、次のとおりである。

作業エリア／プロジェクトチーム	標準化草稿文書	日付	参考文書
D/ CSP 用の信頼できるシステム	電子署名向けの証明書を管理する信頼できるシステムのセキュリティ要件	2001 年 1 月	A２９
F/ 安全な署名作成装置	安全な署名作成装置、バージョン EAL4+'*	2001 年 2 月	A３０
F/ 安全な署名作成装置	安全な署名作成装置、バージョン EAL4*	2001 年 2 月	A３１
G1/ 署名作成のプロセスと環境	署名作成装置のセキュリティ要件	2001 年 10 月	A３２
G2/ 署名作成のプロセスと環境	電子署名検証の手順	2001 年 1 月	A３３
V/ 適合評価	EESSI 適合評価ガイドライン	2000 年 11 月	A３４

* エリア F の CWA 草稿は 2 つの文書からなっている（バージョン EAL 4 とバージョン EAL 4+）

その作業を通じて、CEN/ISSS プロジェクトチームは、その他多数の成果物を開発している。成果物は、次のとおりである。

作業エリア／プロジェクトチーム	ドキュメント	日付	参考文書
D/ CSP 用の信頼できるシステム	一歩前進 － エリア D 担当のプロジェクトチームの範囲改訂	2000 年 11 月	A３５
F/ 安全な署名作成装置	CWA 草稿エリア F に関する意見の新しい整理方法	2000 年 11 月	A３６
F/ 安全な署名作成装置	意見とエリア F の CWA 草稿の解決に関する提案	2000 年 11 月	A３７
F/ 安全な署名作成装置	エリア F の 2 つのバージョンの CWA 草稿に関する説明メモ	2000 年 11 月	A３８
G1/ 署名作成のプロセスと環境	エリア G2 の CWA 草稿に関する意見の新しい整理方法	2000 年 11 月	A３９
G2/ 署名確認のプロセスと環境	エリア G2 の CWA 草稿に関する意見の新しい整理方法	2000 年 11 月	A４０

V/ 適合評価	欧州指令 1999/93/EC の実施のための欧州経済エリア加盟国戦略の一覧	2000 年 8 月	Ａ４１
V/ 適合評価	電子署名の共同体枠組に関する 1999 年 12 月 13 日の欧州議会と会議のの指令 1999/93/EC の条項 3（4）に従って、組織を設計する際に、加盟国が注意を払わなければならない最低基準	2000 年 11 月	Ａ４２
V/ 適合評価	エリア V に関する CWA 草稿に対する意見の新しい整理方法に関する提案	2000 年 11 月	Ａ４３
V/ 適合評価	エリア V に関する CWA 草稿に対する意見の整理方法提案	2001 年 1 月	Ａ４４

1. ***プロジェクトチーム＜エリア D＞：CSP の信頼できるシステム***
   - **議長：**Hans Nilsson, iD2 Technologies（**スウェーデン**）
   - **リーダー：**Wolfgang Schneider ,GMD（**ドイツ**）
   - **専門家：**Farrukh Ahmad, Baltimore Technologies（**英国**）、Jean-Pierre lacombe, Bull（**フランス**）

   エリア D と呼ばれるプロジェクトチームは、認定、登録、許可、リポジトリ、問合わせ能力を含む、認証サービスプロバイダ（CSP）を定義する。現在の定義は、次の機能エリアを含んでいる。証明書発行、取り消し発行、証明書取り消し状態、証明書の配布と登録。オプションエリアには、タイムスタンプ、加入者鍵作成、SSCD（Secure Signature Creation Devices：**署名生成データを実行するために使用される設定されたソフトあるいはハードのこと）作成が含まれている。**

.

2. ***プロジェクトチーム＜エリア F＞：安全な証明作成装置***
   - **議長：**Ricardo Genghini（**イタリア**）
   - **リーダー：**Reinhard Posch, Secure Information Technology Center（**オーストリア**）
   - **専門家：**Wolfgang Killmann, DEBIS（**ドイツ**）、Patrick Salle, Schumberger（**フランス**）

   エリア F と呼ばれるプロジェクトチームは安全な署名作成装置を定義する。装置は、鍵の組を作成する機能を持つことも、持たないこともある。この装置が単なるスマートカードと考えられることもあるので、作業部会は他の装置の使用も検討している。

3. ***プロジェクトチーム＜エリア G1＞：署名作成のプロセスと環境***
   - **議長：**Per Kaijser, Siemens（**ドイツ**）
   - **リーダー：**Robert Willmott, Independent Consultant, Security（**英国**）

・ 専門家：Bruno Struif, GMD（ドイツ）、Adam Balfour, Human Factor Solutions（ノルウェー）

エリア G1 と呼ばれるプロジェクトチームは、署名作成環境を担当している。署名は、以下のいずれかの環境で行われる（a）ユーザが完全に信頼している安全な環境、（b）ユーザが一部信頼している部分的に安全な環境（たとえば、オフィスで個人的用途に雇用者のコンピュータを使う）、（c）信頼できない環境（たとえばパブリックキオスクの使用）。環境は次の 3 つのインタフェースを持つ。ユーザインタフェース、SSCD インタフェース、入出力インタフェース。

4．プロジェクトチーム＜エリア G2＞：署名検証のプロセスと環境

・議長：Ulrike Mueller, BDB（ドイツ）

・リーダー：Denis Pinkas, Bull（フランス）

・専門家：Leonidas Kanellos, 法律家／コンサルタント（ギリシャ）

エリア G2 と呼ばれるプロジェクトチームは、確認環境を担当している。エリア G2 は署名を作成するのに、SSCD を要求せず、ユーザの公開証明書しか要求しない。

5. PT タイトル＜エリア V＞：適合評価

・議長：Richard Wilsher, Zygma Partnership（英国）

・専門家：Jan Sauer, Sauer Quality Consulting（オランダ）、Richard Wilsher. Zygma Partnership（英国）

エリア V と呼ばれるプロジェクトチームは、電子署名の製品やサービスの妥当性確認を担当する。

現在の状況：最近、CEN／ISSS は、２月７日に EESSI に関する会議を開いた。以下の CWA の草稿が E-SIGN ワークショップの承認を受けるために、レビューされた。

・エリア F：署名作成装置、バージョン EAL4 とバージョン EAL4+

・エリア G2：電子署名検証のための手続き

・EESSI 適合評価ガイドライン

エリア D に関する草稿：電子署名の証明書を管理する信頼できるシステムのためのセキュリティ要件に対する意見表明の締め切り日は、2001 年 2 月 23 日である。

３．ＥＥＳＳＩ に対するＥＵ 加盟各国や産業界の反応

（EU ばかりでなく）全世界の政府や産業界によって電子商取引の分野で討議されている主な問題の 1 つは、電子署名と認証機関の問題である。インターネットは本来グローバル

でボーダレスなので、電子署名が関係各国すべてで認められるか、特定の取引によって影響を受けるかが重要な問題である。

すでに、いくつかの国が電子署名と認証機関に関する法律を整備している。また、多くの国では活発に討議されている。電子認証、電子署名、証明書に関する現在の標準化の多くは、ITU グローバル通信勧告、特に ITU-T 勧告 X.509 をベースにしている。さらに、電子署名に対する国際モデル法の開発が、現在 UNCITRAL で進められている。また、国際的な環境で電子署名に適用される一般原則に関してコンセンサスに到達することを目指した、多くの民間イニシアチブも存在している。

このようにすでに複雑な環境において、ＥＵは、電子署名の最初の地域標準化プログラム EESSI を開始した。一般に、EU 加盟政府や産業界は、EESSI を支持している。EU 加盟政府も EU 産業界も、電子商取引のグローバルな性格により、国家証明書の国際的承認に関する適用法と手続き問題が提起されていることを一致して認めている。電子商取引には電子署名標準化の開発での地域協力が必要であり、EESSI は効果的なプログラムであるというコンセンサスが EU 全体に広まっている。

（1）EU 加盟政府内での EESSI の支持

EESSI に対する EU 加盟政府の支持は、1997 年 4 月の欧州委員会の通知「電子商取引での欧州指令」に遡る。欧州議会、会議、経済社会委員会、地域委員会に向けたこの通知で、デジタル署名は、オープンネットワークでのセキュリティを提供し、信頼を築く基本的ツールであると認めた。以後、本閣僚会議などの EU 会議での討議は、電子署名標準化の必要性に関する、EU 加盟政府のコンセンサスを確認した。

この問題に関する委員会の文書も、このコンセンサスを強調していた。「電子通信でのセキュリティと信頼の確保－デジタル署名と暗号化のための欧州枠組に向かって」（参考文書Ａ3）という委員会の報告書を、欧州議会、委員会、経済社会委員会、地域委員会は歓迎した。先に述べたように、委員会は通知を歓迎し、1997 年 3 月に委員会に対してできるだけ早く欧州議会宛ての提案とデジタル署名に関する委員会指令を提出するように求めた。このような経緯で、EESSI は、何ヵ月のうちに明らか EU 加盟政府の間での強力な合意を基にして始められた。

（2）EU 加盟政府内での EESSI に対する懸念

EU 加盟各国政府は EESSI を強く支持している。ほとんどの加盟政府は、電子署名に関する EC 指令を国内法として立法化しようとしている。しかし、EU 加盟政府の中でドイツ政府だけが、この立法化に対して懸念を表明している。

1998 年 3 月に、ドイツ政府は、電子署名に関する EC 草稿指令に対して公式に懸念を表明した。

それは、以下の点に関してである。

・範囲。ドイツ政府は、指令の範囲が広いことを懸念し、「電子署名」ではなくデジタル署名（すなわち、非対称暗号化）に限定することを望んでいる。
・技術標準化。ドイツ政府は、ドイツデジタル署名法を反映するために、指令が提供しているよりも、より詳細な技術標準化を望んでいる。
・責任。政府は、指令で描かれている責任体制がドイツ法と調和しないという懸念を表明している。
・署名者。ドイツ法一般との、そしてドイツのデジタル署名法との調和のために、政府は、電子署名者は、個人（自然人）に限ることを望んでいる。
・手書きの必要性。政府は、電子署名に手書きの署名と同等の法的効力を与える指令の様々な規定に懸念を抱いている。

しかし、ドイツ政府は、電子商取引における電子署名使用のための共通の欧州枠組が必要であるという見解を欧州委員会と共用していることを強調している。また、電子通信での安全と信頼に関して、委員会と 1997 年 10 月 8 日の通知によって導入された電子署名と認証サービスの自由な域内市場のコンセプトを支持している。

また、ドイツ政府は、委員会と欧州議会の共通市場指令は、電子署名の使用の分野における欧州共同体の創設に関する協定の目標にかなう適切な方法であるとの見解を欧州委員会と共用している。ドイツ政府によれば、「ドイツの法、すなわち 1997 年 7 月 22 日のデジタル署名法は、技術的にオープンなコンセプトをベースにしているので、欧州レベルでの指令も、技術的にオープンでなければならず、機能的には、電子的に通信されるメッセージとそのメッセージの完全性の信頼性をベースにしなければならない」。しかし、ドイツ政府は、次のような考えを示している。

「技術的にオープンなコンセプトは、すべての電子署名を指令に含めることを要求しない。むしろ、欧州枠組は、電子商取引で要求される高度な技術的セキュリティ標準を満足する信頼と完全性を保証するデジタル署名（技術コンセプト）に限定されなければならない。これにより、デジタル署名の潜在的利用者に信頼性と法的確実性を与える。電子商取引に有害な影響を持ち、安全でなく、可用性も高くない電子署名につながりかねない技術的中立性を、連邦政府は有用なものと見なすことができない。すでに存在する電子通信や投資の安全性に対する産業界からの高まる要求を背景にして、ドイツ政府は、欧州共通市場で認められる電子署名の高い技術的セキュリティ標準を支持する。セキュリティ標準の主な要素は、できる限り提案されている指令で定義されていなければならない。ドイツ政府は、技術要件の定義が完全に欧州委員会や委員会の手続きに委ねられるのは適当でないと信じている。

提案されている指令は、基本的な欧州の補助的原則に従って、共通市場での安全なデジタル署名の最低限の標準化の調和、認証サービスの自由な流通の必要性、要件に合致しているデジタル署名の相互承認の保証に限定されなければならない。デジタル署名に関する

法的ルールの調和という目的によって正当化されない、加盟各国の責任、証拠、書式に関する法の押し付けを、受け入れられない。欧州デジタル署名に関する認証サービスの共通市場を作るためには、このような法的分野でのいかなる変更も、その絶対的必要性とその範囲を明確に示さなければならないと信じている。ドイツ政府は、指令草稿の検討事項 8 で表明されている法的コンセプトの実施は、この点で満足できるものであると考えている」。

（3）EESSI に関する、EU 産業界の懸念

「デジタル署名と暗号化の欧州枠組に向けて」の公表後に、EC は、加盟各国政府や産業界の支持を取り付けることに努め、加盟各国政府ばかりでなく、民間部門、特に欧州暗号製品業界の代表との会議を開催した。委員会は、関連する様々な民間代表から意見を聴取した。

電子署名や EESSI に関して EU 産業界から、以下のような懸念が表明された。

1. 政府間調整の必要性：複数の加盟各国でのこの分野における法的活動の活発化によって、EU 域内市場の機能に対する重大な障害の発生を防止するために、産業界内部で欧州レベルでの統一した法的枠組が緊急に求められていることが明らかになった。
2. 様々な技術を将来もオープンに：公開鍵暗号を使うデジタル署名技術について多くの議論や作業が存在しているが、EU 産業界は、欧州レベルでの指令は技術中立でなければならず、特定の種類の署名だけに焦点を当ててはならないことを強調している。将来様々な認証メカニズムが開発されると思われるので、この指令の範囲は、データを認証する他の手段ばかりでなく、公開鍵暗号をベースとしたデジタル署名を含む、「電子署名」の層をカバーできるように十分広いものでなければならない。
3. 自主的認定の必要性：EU 域内市場の機能を保証し、ユーザの要求や技術革新での市場の急速な変化に対応するために、EU 産業界は、事前許可を避けなければならないことを強調している。消費者の信頼を得るため、高度なセキュリティを提供する認証サービスプロバイダの自主的な認定スキームも有用であると考えられる。そうした方策が市場によって求められる限り、認証サービスプロバイダと消費者の両方に明確な、あるいは予測可能なレベルの法的安全性が提供される。
4. 契約の自由を確保する：「契約関係がすでに存在しているクローズグループ内で使われる電子署名を、自動的にこの指令の範囲内に入れてはならない。そうしたコンテキストでも契約の自由が存在していなければならない。」等
5. 法的枠組の必要性：電子署名と認証サービスを、特に国際的に、法的に承認することが、この分野での最も重要な問題であると思われる。そのためには、責任を含めて、認証サービスプロバイダの基本的な要件を明確にする必要がある。
6. オープン標準の民間による開発：EU 産業界は、産業界と標準化機関は電子署名の国際的に合意された標準化の開発をリードしなければならないことを強調している。この標準化は、相互運用可能な製品やサービスのオープン環境の確立に焦点を当て

なければならない。委員会の役割は、この過程を支持することであり、リードすることではない。

7. 国際レベルでの調整作業の必要性：国際レベルで、多くの活動や議論が存在している。国際貿易法に関する国連委員会（UNCITRAL）は、電子商取引に関するモデル法を採択し、デジタル署名に関する統一ルールの作成を目指す作業を開始している。経済協力開発機構（OECD）も、1997 暗号化政策のためのガイドラインに続いて、この分野での作業を行っている。その他の国際組織も関連する問題に取り組み始めている。EU 産業界は、現在の開発が欧州レベルでの法的枠組の実装に注意を払わなければならないことを強調している。

実際に EESSI はこうした産業界の懸念のすべてに取り組んでいる。

（4）EU 産業界以内での EESSI の支持

EU 産業界は、EESSI を強力に支持している。この支持は、公認の欧州標準化機構（ESO）、すなわち欧州通信標準化機構（ETSI）、欧州標準化委員会の使用によって表明されている。これらの ESO は、EU 産業界のメンバーから構成されている作業部会を基にしている。これにより、EESSI によって開発される標準は、電子署名の分野に関与している大手の EU 企業からの支持が得られる。

たとえば、EESSI は、ICT 標準化会議、ETSI、そして CEN 内の EU 産業界の活発な関与をベースにしている。これらの組織に関与している企業には、電子商取引の分野の先進的な EU 企業が含まれていて、たとえば、次の企業を挙げることができる。

- Baltimore Technologies
- BDB
- Bull
- DEBIS
- GMD
- Human Factor Solutions
- id2 Technologies
- Schumberger
- Secure Information Technology Center
- Security & Standards Consultancy
- Siemens
- Telia Research
- Zygma Partnership

その他数百の EU 企業も、ICT 標準化会議への業界団体の参加を通じて EESSI に代表を送っている。

・ATM フォーラム
・デジタルビデオ放送（DVB）プロジェクト
・欧州家電メーカ協議会（EACEM）
・欧州放送連合（EBU）
・欧州バンキング標準化委員会（ECBS）
・ECMA
・ERTICO インテリジェント輸送システム-ヨーロッパ
・TeleManagement フォーラム（元 MMF）
・オープングループ
・オブジェクトマネージメントグループ（OMG）

EESSI に対する EU 産業界の支持は、EESI 標準化草稿の開発において ETSI や CEN の作業を取り込んだ、多くのオープン会議を通して拡大した。

しかし、EESI はまだ標準化作業の大部分をまだ完成していないので、EESSI に対する EU 産業界の支持の最終レベルを判断するのは早計である。

第２章 イギリスの電子署名関連の法律および規則

電子署名に関するイギリス国内法令については、過去数年間にわたって発展している。法令の最も新しい段階は、1997 年に始まった。この年にイギリス政府は、貿易産業省を通じて「信頼できる第三者機関の認可に関する協議」に着手した。この分野における政府の法令策定作業は、その後数年にわたって進行し、2000 年に電子通信法が制定されるに至った。この法律に基づいて、明確な形で電子署名が法的に認められた。

電子署名の利用を推進するため、イギリス政府は、産業界側の「自己規制承認」制度策定に同意を与えて、最低限の品質・サービス基準を確保しようとした。この自己規制制度が効果的に運用されれば、イギリス政府が法定制度を構築せずに済む。産業界主導型の電子署名評価機関は、「tScheme」と呼ばれている。この機関は、イギリスや欧州連合の法令に基づいた非営利団体として活動する予定である。tScheme は、依然として計画段階にある。2000 年 11 月に、初めて「tScheme 認可要領」（4 件）が tScheme 暫定理事会によって承認され、その内容がパイロット・プロジェクトとして公表された。2001 年 3 月以前に完了予定のパイロット・プロジェクトは存在しない。将来的には、サービスが tScheme 理事会によって承認されると、その旨の告知が認定サービス要覧で公表される。

本章では次の項目に関して報告する。

１．電子署名の分野における政府の役割および機能
２．電子署名に関する最近の法律および規則
３．電子署名関連の法律と規則に対する産業界の反応

１． 電子署名の分野における政府の役割および機能

イギリス政府の立場は、電子商取引が注文、資金その他のコミュニケーションの国際的移動を推進するので、電子商取引が国際的に極めて重要な役割を果たすというものである。したがって、電子商取引分野においてある国が施策や政策を実施すると、他国との貿易に影響が及ぶだけでなく、他国間の貿易にも影響が及ぶ可能性があるという命題をイギリス政府は支持している。そのため、これまでのイギリス政府の立場は、電子商取引に対する法的・技術的なアプローチが一致していなければ、国際貿易の大きな障害につながるという考えで一貫している。このような流れを受けて、イギリス政府は、電子商取引に対して以下の政策を想定している。

・ 政府の役割・機能とは、電子署名の利用を推進する国内法令を企画立案・執行して、電子商取引を促進すること。
・ イギリス政府は、国際的な電子商取引を推進できる範囲内で、国際的な標準化作業と国内法の調整作業を支援する。

電子署名政策に関する政府機関

イギリス政府は、主要政府 2 機関（貿易産業省と通信電子セキュリティ・グループ）に対して、電子署名法令に関する実際の策定・実行権限を委任している。

- 貿易産業省（DTI）は、電子商取引に関するイギリス国内法令の企画立案と実施を担当している。
- 通信電子セキュリティ・グループ（CESG）は、政府の IT 通信システムの安全性を確保する技術的側面を監督することである。

２．電子署名に関する最近の法律および規則

1996 年に「公共ネットワークにおける暗号利用に関する規制目的」が公表された後、貿易産業省は一連の政策ペーパーを公表するとともに、電子署名の問題について、イギリス産業界との間で繰り返し協議の場を設けた。このような取り組みを経て、2000 年電子通信法が制定されるに至っている。

（1） 1998 年 － 安全な電子商取引に関する声明

1997 年の TTPs ペーパーに関する協議期間が終了した後、貿易産業省は、1998 年 4 月に議会に声明文を提出した。そのタイトルは、「安全な電子商取引に関する声明」（参考文書 B4）であった。この声明では、以下の諸点に関して、強制的制度よりも「自発的」認可制度を推進する法制度が必要であるという認識が述べられている。

- 認定機関と「信頼できる第三者機関」に関すること
- 通常署名と同等程度に電子署名を認定すること
- 通信内容や保存データの解読に必要な情報に対して合法的にアクセスできるよう、警察当局が令状を取得できること

この声明において、貿易産業省は、最終的に上記の諸問題に関する法制度を導入する意思がある旨を正式に表明した。この法案の内容は、「認可を受けた認証機関によって作成された署名が法的に認められると推定」することによって、電子署名の法的な地位を確立するものであった。法案は、1998 年 11 月に提出される予定であった。しかし、貿易産業省はこの期限内に法案を策定できなかった。その代わり、貿易産業省は別の協議用ペーパーを公表した。

（2） 1999 年 － 電子商取引の信頼性構築

1999 年 3 月に、貿易産業省は、「電子商取引の信頼性構築」と題する電子商取引に関する協議用ペーパー（参考文書 B5）を発表した。このペーパーでは、主に電子署名が取り上げられている。当時、イギリス政府は、国内法の改正について 2 種類の方法を検討していた。

1) 主要法令において、署名と文書に関する法律上の要件をそれぞれ改正する。
2) 主要法令を活用して、政府が個別具体的に規則を修正できるようにして、電子署名や電子文書を法的に認定する。

さらに、法律を通じて、一定の条件を満たす電子署名（認可を受けた認証機関によって認証された電子署名）がその署名者の同一性を示すという推定を設ける旨の政府の意図が公表された。

「電子商取引の信頼性構築」（参考文書B5）では、以下の諸点が記載されている。

- 国際的関連性
- 法的問題
- 法律上の要件
- 認可体制
- 警察当局の関心事項
- 業界の提携
- 認可交付基準

新しく協議期間が設けられ、この協議期間は1999年4月1日に終了した。このような期間を設けた目的は、イギリス政府の政策実施に関する詳細事項について、意見を聴取することであった。この協議から教訓を得る形で、貿易産業省は、電子商取引法の最終案を提出した。

（3） 2000年 ― 電子通信法

1999年11月に、貿易産業省は電子通信法案（参考文書B6）を下院に提出して、その審議を求めた。2000年5月に、同法案が正式にイギリス法になった。この法律では、以下の事項が規定されている。

- 電子署名は、裁判所によって明示的に法的認定が与えられている。
- 紙の使用を義務付ける既存法令の障壁は、今後、可能な部分から改正される。
- 自発的な「自己規制認可」制度を設けて、最低限の品質・サービス基準を確保する。
- 上記の自己規制制度が実効的に運用されれば、政府が法定制度を構築することもない。自己規制制度が機能不全に陥った場合に限って、政府は法定制度を構築するが、そのような場合であっても自発性は維持される。法案のこの部分については、「サンセット条項」が適用される。法定制度が5年以内に成立しない場合、政府が法定制度を確立する権限も消滅することになる。

法案審議期間中に、政府は企業やIT産業と幅広く協議を実施したことを踏まえて、以下の修正を行った。また、政府が発表した内容は、以下の通りである。

- 強制的なキー・エスクロー制度は、法案から削除される。

・ 重要な捜査権限については、この法案から内務省の「捜査権限法」に移管される。なお、捜査権限法については、関係法案の総合的改正と並行して、審議される予定である。

最終的に同法は以下の 3 部構成になっている。

第 I 部 － 暗号サービス業者

電子通信法案の第 I 部は、暗号サービスの提供業者を対象とする自発的法定認可制度について記述している。tScheme の策定を受けて、第 I 部は施行されていない。

（条項）

1） 認可業者の登録
2） 認可交付に関する制度
3） 認可機能の委任
4） 情報開示に関する制限
5） 第 I 部に基づく規制
6） 暗号支援サービスの提供

第 II 部 － 電子商取引の推進、データ保存

法案の第 II 部には、電子的な方法を提供することによって電子商取引を推進する規定が盛り込まれている。この方法は、従来型のデータ通信・保存方法の転換で利益を得られる者のみによって利用される。政府は、本法案の第 II 部を介して 1985 年会社法を改正し、企業が電子媒体を利用できるようにして、社内通信の提供、株主の議決・委任状の受理、法人設立を可能にしている。 政府の試算によると、年次報告書の印刷・配布に関する費用節約だけを見ても、株主が電子的手法を利用した場合、株主 1 人あたり 10 ポンドに達するという。

（条項）

7） 電子署名および関連証明書
8） 法律改正権
9） 第 8 条の命令

第 III 部 － 雑則・補則

法案の第 III 部によって、認可修正（注）プロセス（1984 年電気通信法第 12 条で詳細に規定）が簡素化されている。

（条項）

10） 長官による認可の修正
11） 認可取得者の同意を得ていない場合の修正に対する不服申立
12） 省庁の支出等
13） キー・エスクロー要件に関する禁止事項
14） 一般的解釈
15） 略称、適用開始、適用範囲

貿易産業省の「電子通信法案に関する規制の影響評価」（参考文書B8）では、主に以下の諸点が検討されている。

- 電子通信法の利点
- 企業から見た法令遵守費用
- 執行、制裁、監視および審査に関する諸手続

＊注：この法案には、電気通信認可の修正手続を改正する権限が盛り込まれている。元来、現行手続は、認可保持者が少数である場合を想定しており、認可保持者が多数になった場合には不適切な内容になっている。業界との協議を経て、この手続が簡素化されているので、市場状況に即した形で容易に認可内容を修正できるようになる。

（4） 国際的立場

国際的に見て、貿易産業省は、EESSI プログラムを支持している。また、UNCITRAL（国連国際商取引法委員会）や OECD（経済協力開発機構）の電子商取引を支援する活動も支持している。

- EESSI（欧州電子署名標準化構想）は、欧州共同体電子署名命令に基づく活動の第 1 段階を完了している。
- UNCITRAL は、電子商取引に関するモデル法案を公表しており、電子署名統一規則の原案も存在している。
- OECD は、「暗号政策 ― ガイドラインと諸問題、情報システムのセキュリティに関するガイドライン」を発表している。1999 年 2 月、OECD は電子署名の活動を行うことに同意している。

３．電子署名関連の法律と規則に対する産業界の反応

電子通信法は、産業界と政府の間で数年間にわたって議論を展開してきた結果、生み出されたものである。上述したように、1997 年協議用ペーパー「暗号サービスの提供に関する信頼できる第三者機関の認可交付」を公表した後、政府は産業界から激しい批判を受けた。しかし、産業界と政府との間で 3 年間にわたって協議を実施した結果、イギリスでは幅広い支持を受ける形で法制度が生み出された。政府・産業界の協議を通じて、政府は、業界側の懸念事項の大部分に対応してきた。このような事情を受けて、イギリス産業界は、最終法案を支持するに至っている。

- 「電子商取引に関する信頼の構築」（参考文書B9）
- 「電子商取引協議の推進」および「電子通信法案」（参考文書B10）

(1)　電子通信法に対する企業の支持

電子通信法を明確に支持している企業としては、以下のものが挙げられる。

・ カレン・トムソン氏（AOL UK 代表取締役）は、「これまで AOL は、メンバーが簡単かつ安全にオンライン・ショッピングできるように活動を展開してきた。電子通信法を通じて電子署名が法的に認められることにより、電子商取引の範囲が広がって、電子媒体に対するメンバーの信頼性も向上することになる」と述べている。

・ ジョン・ブラウニング氏（First Tuesday 社の共同設立者）は、「信頼関係はビジネスを成功させる上で最も重要な基盤である。新型のインターネットはイギリス経済や世界経済で大きな役割を果たしているが、少なくとも電子分野の一貫性、予測性と信頼性を物理的分野と同様のものにするよう法環境を整備することは、これらのインターネット企業を政府として支援する活動の中でも、最も重要なものである」と語っている。

・ カール・シモン氏（IBM United Kingdom Limited 社最高経営責任者）は、「IBM としては、この重要施策の導入を歓迎しており、新世紀初頭に法案が成立すると期待している。法案の文言を見れば、政府が業界の意見に注意深く耳を傾けていることは明らかである。特に、新しい技術やサービスの信頼性構築に向けて、担当大臣が業界主導型アプローチを支持しているので、大変嬉しく思っている。イギリス産業界がこの構想を前進させて、イギリスにおける電子商取引のニーズに対応するだけでなく、ヨーロッパや世界の諸国に対して模範例にしなければならない」と述べている。

・ デビッド・スベンセン氏（Microsoft Ltd.社会長）は「本日、法案が公表され、この法案の中にヨーロッパ諸国が準拠すべきモデルケースが盛り込まれている。このことを見れば、今後、イギリスが電子商取引に最も適した場所になるというメッセージをイギリス企業やヨーロッパ企業に対して送ることになる」と語っている。

・ キース・トッド氏（ICL 最高経営責任者）は、「これは朗報である。正当な商取引の問題が警察権力の問題から分離されている点を特に歓迎したい。なぜなら、政府が業界の意見に耳を傾けている姿勢が明白であるからだ。ICL は、自己規制制度の策定面において電子ビジネス同盟に貢献しており、この自己規制制度は法案の第Ⅰ部の要件を満たしていると理解している。このような形で新しい産官提携が実現することにより、イギリスが電子商取引に適した場所になるだろう」と述べている。

・ キース・チャップル氏（Intel UK 社代表取締役）は、「政府が法案の中で、キー・エスクロー制度の削除を確認したことや、電子署名の法的認定という問題を重視したことについて、大変嬉しく思う。これにより、企業や消費者の信頼性が大きく向上するだけ

でなく、イギリスにおける電子ビジネスの拡大にも寄与することになるだろう」と述べている。

・ InterClear 社（イギリス最大の民間電子認証機関）は以下の声明を発表している。「InterClear 社としては、先日、政府が電子通信法案を公表したことを歓迎している。なぜなら、この法案を発表したことを通じて、安定的な環境が構築され、その結果として、電子事業の成長が推進され、世界市場におけるイギリスの地位も強化されるからである。特に重要な点として、本当の意味で電子ビジネスを実現するには、信頼性が極めて重要な役割を果たすと政府が認識し、その結果、電子証明書を裁判所に証拠として提出できる旨を政府が決定したことがある。それとは逆に、この法案では、すべての電子証明書が等しい効力を持っているとは認定されていない点も重要である。したがって、各電子証明書の価値は個別具体的に裁判所が判断する問題ということになる。」

・ボブ・カーター氏（InterClear 社代表取締役）によると「協議プロセスでは幅広い問題が取り上げられ、時として激しい議論も展開されたが、InterClear としては、この法案が成立することでイギリスの電子ビジネス環境が高度に整備されると確信している。また、電子政府構想を通じて政府がますますリーダーシップを発揮すると思われる。電子証明書の価値というものは、信頼構築のプロセスや関連設備が発行に有利なものか否かによって左右されるというのが政府側の認識である。すべての証明書の地位が等しい訳ではない。したがって、重要なのは、エンドユーザー側で自分が利用する証明書の価値を理解し、自分達、その顧客や取引先が証明書に与えている信頼性を完全に管理できるようにすることである。また、電子証明書の商業的な価値や有効性をさらに担保するには、電子商取引法案では、この分野における自己規制制度が最も現実的な解決策であると認識されている。tScheme 構想の設立メンバーとして、InterClear 社はこのような展開で最前線に立って大きな役割を果たしている。tScheme を通じて、法的拘束力のある通信手法を目指して、電子証明書の発行・管理方法に関する業界標準が具体化されることになるだろう」と述べている。

（2） 電子通信法に基づく法改正に関する産業界側のコメント

電子通信法に基づいて、貿易産業省は 1985 年会社法も改正して、同法に基づく電子通信の利用に関する規定を設けた（参考文書B12, B13）(注)。

＊注: 電子通信法案には、電子通信の利用を妨げる障壁が存在する場合、政府が電子通信手段を推進できる旨が規定されている。

電子通信に関する貿易産業省の協議書簡に対する産業界側の反応 － 1985 年会社法の改正については、支持する姿勢が大勢を占めていた。このようなコンセンサスに基づいて、イギリス政府は、以下の施策を実施することになっている。

1）同法に基づいて企業が社員に送信しなければならない文書については、社員が同意を与えている場合に、（欧州共同体の制約条件に基づいて）社員が指定したファックス番号または電子メールアドレスに対して送信できるようにする。同法によって義務付けられた社内通信については、関連情報の受信資格がある者がアクセスできるウェブサイトその他の電子的サイト上に企業が掲載できるようにする。また、社員が同意を与えている場合に、その社員に対して直接通信内容を送信する代わりに、その社員によって指定されたアドレスに向けて利用通知のみを送信できるようにする。

2）会社がその旨の決定を下した場合、委任状の指名を会社に返送する場合、書面、ファックスまたは他の電子的手段により、その効力を発生できるようにする規定を設ける。

3）電子的手段を用いてカンパニーズハウス（Companies House：政府の一部門）に企業を設立の手続ができるようにする。

第3章 イギリスの評価機関

本章では暗号評価に関連する 2 機関について取り上げる。

1．The Department of Trade and Industry （DTI）貿易産業省

2．The Communications-Electronic Security Group （CGSG）通信電子セキュリティ・グループ

貿易産業省（DTI）は、電子署名に関するイギリス国内法令の企画立案・実施を担当しており、同省の主管法令としては、電子署名に関する現行法令、2000 年電子通信法などが挙げられる。同法に基づけば、貿易産業省は、電子署名製品やサービスの提供業者を直接的に評価しない。むしろ、貿易産業省は、産業界側が法令に基づかない形で自発的・自己規制型機関を設けて電子信用サービスを認可する同意している。この合意は、tScheme と呼ばれている。イギリス電子ビジネス同盟（AEB、イギリス企業協会の共同体）が tScheme 合意を担当している。イギリス電子産業連盟が、プロジェクトの指揮監督を行っている。

対照的に、CESG（イギリス政府通信本部の一部）は、イギリス政府の技術系政府機関であり、暗号の公式利用（政府による利用）を担当している。通信電子セキュリティ・グループの職責は、政府の IT 通信システムの安全性を確保するような技術的側面を監督することである。

1． 貿易産業省と tScheme

貿易産業省（DTI）は、イギリス政府の省庁であり、その使命は、「競争力と科学的優位性を増して、現代経済における持続的成長と生産性を強化する」ことである。

貿易産業省（以前の名称は、商務局）は、その長い歴史を通じて、幅広い職務を担当してきた。その一例として、電子署名に関するイギリス国内法令の企画立案・実施が挙げられる。

ここでは以下の項目を報告する。

（1） 貿易産業省の組織構造

（2） セキュリティ製品に関する貿易産業省の評価プログラム（Defunct）

（3） 電子通信法に基づく電子信用サービスの承認を担当する自発的・自己規制型機関に関する貿易産業省の合意（tScheme）

（4） tScheme の運用方法

（5） tScheme のパイロット・プロジェクト

（6） tScheme の最近の活動（プロファイル案およびガイドライン案）

(1) 貿易産業省の組織構造

現在の貿易産業省の組織構造は、1983 年 6 月以来のものである。当時、イギリス政府は、貿易省と産業省を統合する決定を下した。新しく設けられた省庁（貿易産業省）は、産業省の産業担当部門と、貿易省の商取引関係・貿易部門を統合したものである。また、貿易産業省は、内務省からラジオ周波数規制権限を獲得する一方で、民間航空・海運関連の職務を運輸省に移管した。

電子商取引の分野に関して、貿易産業省は、その職務を通信情報産業（CII）理事会に委任している。CII は、主に 3 種類の役割：具体的には、出版・情報、電子・通信技術やサービスセクターの支援、これら技術の利用推進、規制の実効性確保を果たしている。

(2) セキュリティ製品に関する貿易産業省の評価プログラム（Defunct）

1987 年に、貿易産業省は、商用コンピューター・セキュリティ・センターを設立して、市販の IT 製品に対する公式セキュリティ評価の適用を検討させることになった。その結果、運用に関する一連の評価基準と概要計画が「グリーン・ブック」という形で公表された。これらの基準については、1989 年に審査が行われ、産業界側との間でも幅広い協議の場が設けられた。さらに、イギリス政府と産業界は、一元的な制度を設けることで利益が大きくなるという点で認識が一致し、この流れを受けて、1989 年 12 月に CESG と貿易産業省の新合同制度が公表された。なお、この新制度は、イギリス IT セキュリティ評価認定制度と呼ばれており、通常、「イギリス ITSEC 制度」という略称で呼ばれている。この制度は、1990 年 7 月 4 日に開始され、1991 年 5 月 1 日に本格稼動を開始した。

(3) 電子署名に関する貿易産業省の評価プログラム － tScheme に関する産業界の同意

電子通信法に基づく電子署名技術の評価に関して、貿易産業省は、業界側との間で合意を成立させて、電子信用サービスの認可に関して、法令に基づかない形の自発的・自己規制型機関を業界側が設けることになった。この合意は、tScheme と呼ばれている。

イギリス電子ビジネス同盟（AEB）が tScheme の組織構成を担当した。イギリス電子ビジネス同盟は、5 大企業連合の集合体であり、イギリスの電子ビジネスに適した競争環境の推進を目指している。5 大企業連合の名称を列挙すれば、以下のようになる。

- イギリス産業連盟（CBI）
- 電子産業連合（FEI）
- 直接販売協会（DMA）
- コンピューター・サービス・ソフトウェア産業組合（CSSA）
- イギリス電子センター

このなかで電子産業連合は、tScheme の企画立案作業で主導的な役割を果たしている。

イギリス産業界は、tScheme のコンセプトを積極的に支持している。電子ビジネス同盟は、「電子通信法が施行されたことは、企業にとって追い風になる。その一方で、電子署名が認定されたことにより、信頼性が構築され電子ビジネスも推進されるだろう」という見解を示している。

アンソニー・パリシュ氏（電子産業連合会長）は、「政府が業界の意見に耳を傾けるとともに、新しい技術やサービスの信頼性を構築する最適な方法として自己規制アプローチが認識されたことは、大変嬉しく思う。法令に基づく認可の留保権に関して「サンセット」条項が挿入された背景には、実効的な自己規制を支持している政府の姿勢が示されている」と述べている。

（4） tScheme の運用方法

イギリス産業界は、信用サービス業者の規制に関して、強制規制を回避したいと考えていた。当初の法案には、法定規制制度に関する規定が盛り込まれていたが、1999 年に、電子通信法が成立する前、イギリス電子ビジネス同盟は、貿易産業省に対して、法令に基づかない制度である「tScheme」に関する概要を提示した。これにより、電子信用サービスの認証に関して、信頼性・効果性の両面で優れた制度や手続が設けられることになった。

tScheme は、独立した非営利団体であり、電子信用サービス業者を対象とする共同規制制度として設立された。tScheme は、会費や手数料を通じて自力で運営資金を調達している。また、イギリス国内法や欧州連合の法規に基づいて業務を展開しており、暗号や関連電子サービスを幅広くカバーしている。ユーザー、業者、技術系企業を代表する諸団体が主体となって活動を展開しており、出身母体も、産業界、政府、同業組合、消費者団体など多岐にわたっている。tScheme が規制環境を提供することを受けて、2000 年電子通信法に基づいて貿易産業相の権限行使は回避された。

tScheme の公式の役割は、以下の通りである。

- 暗号サービス（電子メールの送信者受信者や蓄積データのため、また暗号技術を使用するように設計されたサービス）を対象とする自発的認定に関して、電子通信法案の要件を満たす。
- 認証・監督に関する欧州共同体電子署名命令の要件に対応する。
- 信用サービスのユーザー（企業、政府、消費者）側のニーズと業者側のニーズを考慮に入れる。
- 認可を受けた信用サービスの運用状況を監督するとともに、適切な是正メカニズムを提供する。
- 業界主導型・市場指向型でオープンな基準の導入に関して主導的な役割を果たす。
- 電子商取引の実施に関してイギリスを模範例にするという政府と業界側の要望を側面支援する。

・ 国際的な状況や展開を考慮に入れる。
・ 認定を受けた信用サービスや関連技術の利用を推進する。

tScheme は、いまだに稼動するには至っていない。電子産業連合の監督下で企画立案作業が進行しており、その結果、tScheme 暫定理事会が設けられた。このような事情を受けて、運用方法の詳細については、未知の部分が多いが、原則論としては以下の諸点が挙げられる。

・ 電子信用サービス業者が信頼に足ると判断される場合、その業者の運用基準について、tScheme が定義する（この基準は、プロファイルと呼ばれている）。
・ tScheme は、上記の定義を公表するとともに、信用サービス業者に対して、妥当なプロファイルに照らしてサービス内容を評価する機会を設ける。
・ TSP によって提供されるサービスが tScheme 理事会によって認可されると、tScheme 品質保証マークに示された信頼性のレベルが達成されたと見なされる。
・ 上記の通知は、認定サービス要覧において公表される。
・ サービス業者が品質保証マークを利用する場合、業務内容の質を維持するため、是正措置や制裁措置に関する契約条件に拘束される。

現時点において、完全な形で認可を受けた信用サービスは存在しない。なぜなら、現在進行中の tScheme パイロット・プロジェクトのうち、2001 年 3 月以前に完了予定のものは存在しないからである。

(5) tScheme のパイロット・プロジェクト

パイロット・プロジェクトの実施目的の一つとして、認可プロファイルおよびガイドラインで規定された認可基準の実効性を判断することがある。パイロット・プロジェクトにおいては、信用サービス業者と UKAS（英国認証機関認定審議会）が共同して活動を展開している。UKAS は、検査基準試験場および認定検査機関の認定に関して、イギリス政府によって唯一認可された全国的組織である。非営利団体である UKAS は、保証契約によって活動範囲が制限されているが、貿易産業省を通じて、政府との覚書に基づいて活動を展開している。

UKAS の（サービスプロバイダ、個人、組織や団体に関する）認証プロセス

・申請 － まず、予備申請を行って、指定の申請書を用いて UKAS に申請手数料を沿えて提出する。その後、関連書類を同封した申請書類一式が送付されてくるので、評価要請と詳細部分を照らし合わせて評価準備の参考にする。

・評価要請 － UKAS が評価申請書と所定書類を受理して検討を行った後、評価担当者が割り当てられて、この評価担当者が提出書類を検討する。評価担当者から連絡が来た

時点で、事前評価視察と評価チームの構成について協議を行う。

・事前評価視察 ― 一般的に、UKAS は、UKAS の評価担当者または首席査定官による非公式事前評価視察を推奨している。この視察では、要請対象となった認証の範囲が確定される。通常、事前評価では作業日数で延べ 1 人～3 人の労働力が投入され、申請者が評価全体を実施できる状態か否かが検討される。

・第 1 回評価視察 ― 正式な評価は、通常、評価担当者によって実施され、評価担当者の指揮下で、認証範囲の専門知識を有する独立技術査定官が活動する。視察期間は、要請された認定範囲によって左右される。認定要件に合致していないことが判明した場合、評価視察期間中にその旨が書面で通知され、その問題の解消方法に関して UKAS に通知するよう求められる。問題点が解消され、UKAS がその旨を認めると、認定を受けられることになる。

・認定の管理 ― 認定については、調査視察を通じて年に 1 回、その内容が確認される。完全な再評価は 4 年に 1 回実施される。

・認定範囲の拡大 ― 任意の時期に認定範囲を拡大できるが、実行中の調査プログラムの一環として範囲の拡大が評価されている場合、費用を抑えられる。査定官や事務処理時間を増やさなければならない場合、範囲拡大に関する追加手数料が徴収される。

・グループ認定 ― グループ認定は、同一団体における研究所や事務処理センターを一括して認定する行為である。対象となるのは、共通の品質制度や共通の品質管理に基づいて、統一的に活動している団体である。

・不服申立 ― UKAS の認定決定（または、通知を受ける団体の法的地位の提言に関する決定）に同意できない場合、その決定に対して不服を申し立てられる。不服申立は、まず UKAS の職員によって検討される。この内部プロセスを通じて問題点が解決されない場合、第三者評価機関が申立案件を審査する。

・認定費用 ― 事前申請を行い、UKAS に申請手数料（2000 年 4 月 1 日以降、600 ポンドと付加価値税）を沿えて申請書を送付した後、2 年以内に品質マニュアルを添えて、評価申請書を UKAS に返送しなければならない。この期間を経過すると、申請書の検討結果が無効になったと見なされる。その後になって評価を受ける場合、UKAS に再申請を行って、別途、申請手数料を支払わなければならない。

・UKAS に関する他の手数料は、「延べ作業日数」料率を用いて個別具体的に決定され、第 1 回評価の実施や（認定後における）認定の維持に必要なスタッフや査定官の作業内容を基礎として計算される。評価チームの規模は、認定の複雑性や範囲に応じて変化する。この作業では、現場や事務所での作業に加えて、報告書の事務処理作業なども行われる。

・UKAS の現行「延べ作業日数」料率（1999 年度～2000 年度）は、研究所関連作業が 604 ポンド（出張費を含む)、認定機関関連作業が 726 ポンド（出張費を除く)、検査機関関連作業が 767 ポンド（出張費を含む）になっている。

・移動時間は、作業日数の一部として含まれるが、国際出張や遠隔地の場合には、例外として追加移動時間が加算される。認定視察と海外視察については、出張費が個別に徴収される。

・UKAS は、視察に先立って、評価や年次調査に関する見積を提出している。視察が行われる前に、企業は手数料を承認するか否か確認しなければならない。

（6） tScheme の最近の活動（プロファイル案およびガイドライン案）

2000 年 11 月 1 日、tScheme 暫定理事会は、認可プロファイルおよびガイドラインに関する原案（4 種類）を承認した。これらのプロファイルおよびガイドラインは、現在進行中のパイロット・プロジェクトで利用できるよう、文書化作業が進行している。

- 登録サービスに関する認可プロファイル（参考文書B16）
- 個人の身元確認に関するガイドライン（参考文書B17）
- 団体の身元確認に関するガイドライン（参考文書B18）
- 基準認可プロファイル（参考文書B19）

これら 4 件の認可プロファイルおよびガイドラインについては、tScheme プロファイル策定プログラムを通じて策定作業が進行している。これらの文書には、tScheme 認定品質保証マークの導入・利用から利益を受けている場合、電子信用サービス業者を監査する場合の認可基準が記載されている。

- 公表後の認可プロファイルやガイドラインは、必要に応じて改正される。改正後の内容は、tScheme 理事会の承認を受けた後、従来の内容に代わって効力を発生する。

- プロファイル追加策定作業は、品質証明書に関する信用サービスを重視する形で実施されている。策定作業中のプロファイルの具体例としては、鍵保存プロファイルなどが挙げられる。

tScheme サービスのユーザー（この場合のユーザーには、関係者も含まれる）や提供業者の双方にとって、認可プロセス全体をできるだけ簡素化するため、「ウェブ・ブック」が策定されている。この「ウェブ・ブック」には、各サービスの認可に必要な関連情報や関連プロセスが網羅的に記載されることになっている。

2．通信電子セキュリティ・グループ(CESG)

通信電子セキュリティ・グループ(CESG)はイギリスの行政サービス部門の一部であり、公式な政府機関である。具体的には、CESG はイギリスの政府通信本部(GCHQ)の正式な一部門である。CESG は、GCHQ と同じく、議会による公式の監督下に置かれているが、機密保持の役割を持つグループとしての役割を担っている。

ここでは、CESG に関する下記の情報について報告する。

（1） CESG の組織構造
（2） CESG のガイダンス
（3） CESG の評価方法
- CESG 支援製品化計画(CAPS)
- IT セキュリティの評価と認定(UKITSEC 計画)
- CESG がリストするアドバイザー計画(CLAS)
- IT ヘルス・チェック・サービス(CHECK)

（4） CESG が承認し、ITSEC が認定した製品のリスト
（5） その他の CESG のプログラムと製品

（1） CESG の組織構造

CESG は、イギリス政府による暗号方式の公的使用ならびにより全体的な情報セキュリティ(Infosec)（注）に関する任務を受け持つ政府の国立技術機関であり、公的な IT および通信システムの危機を技術面から守ることをその職務としている。CESG は下記により Infosec を実行している。

・情報セキュリティに関するイギリス政府の政策決定を補佐する。
・政策実施にあたり政府および民間セクターの公的ユーザーに対するコンサルタントとして全般的なアドバイスを行う。
・政府が使用する暗号製品(音声を暗号化する「暗号電話」など)の開発を行う。
・政府の使用に適した暗号製品のための産官共同での民間の開発者を支援する。
・ 訓練コースを運営する。
・政府の暗号化製品およびシステムのための消耗品を提供する(Keymat)。

＊（注）CESG が使用しているように、「Infosec」という用語は、コンピュータ・セキュリティ(Compusec)、

通信セキュリティ(Comsec)、電磁波セキュリティ(Radsec)の総称である。

CESGの主なサービス対象先はイギリス政府(HMG)の各省庁およびイギリス軍だが、過去10年間に情報技術が進歩し、政府全般にわたり“情報セキュリティ”の採用が増大したことから、CESGのサービス対象範囲はかなり拡大した。またたとえば、CESGは省庁に属さない公共団体および他の公共セクター機関およびイギリス警察にサービスを提供し、さらにCAPS、CLAS、CHECK、およびITSEC計画等でイギリス商工業界との接触も持っている。しかし、CESGの第一の目的は、民間セクターに評価および、または認可サービスを提供することではなく、むしろイギリス政府の情報セキュリティのニーズに応えることにある。

CESGは顧客を特定したサービスおよび製品について費用回収の原則で運営されている。Infosec政策および同標準に関する文書は、イギリス官界のほとんどに無料で提供されるが、その他の製品やサービスは有料である。

(2) CESGのガイダンス

イギリス政府の情報セキュリティに関する技術機関として、CESGは最新のガイダンスと基準を必要とする部署向けに確実に提供する重要な責任を負っている。この仕事は、すべてのイギリス政府省庁を利する「公益」活動として管理される。CESGの発行する全般的Infosecガイダンスの多くは地方自治体や同様の公共セクターにも適用される内容である。

CESGメモランダム・シリーズは、重要なInfosecトピックスのいくつかを紹介する文書であり、イギリス公共セクター(政府省庁、軍など)内の情報処理者はこれらを無料で入手できる。現在発行されているCESGガイダンスには下記のものがある。

- 政府のインターネット接続安全化への助言
- 秘密情報に使用したコンピュータ媒体の処分法
- 大規模ネットワークに関するセキュリティのニーズの評価、ITシステムのセキュリティ対策を文書化する方法
- 公開鍵暗号方式使用の認証と保全性
- パスワードの正しい管理法
- 公的データに関する技術的危険要因
- 電磁波セキュリティ(TEMPEST)の問題

(3) CESGの評価方法

通常、CESGはセキュリティ装置を製造することはないが、公的ニーズを満たし、広範囲に利用できる製品およびサービスを入手するため、そしてそれらのサービスを下記のプログラムでサポートするインフラストラクチャを整備する上で産業界と緊密な連携を保っている。

a) CESG 支援製品計画(CAPS)
b) IT セキュリティの評価および認可(UK ITSEC 計画)
c) CESG がリストするアドバイザー計画(CLAS)
d) IT ヘルス・チェック・サービス(CHECH)

a) CESG 支援製品計画(CAPS)

CESG 支援製品計画(CAPS)は、セキュリティ製品をイギリス政府向けに商業上のリスクも負って開発する企業のための会員制の計画である。年会費を収めると、企業は CESG の知識、技術力、および Infosec の分野での経験を利用することができ、またある種のサービスを直接受けることも可能である。

この計画に参加する会員は、適切な CESG 暗号アルゴリズム（イギリス政府が使用するために政府自身が開発した暗号アルゴリズム、*Thames Bridge*、*Red Pike* という名称のアルゴリズムがある）をイギリス政府に納入する自社の製品に使用し、 CESG の評価を受けることができる。認可が得られると、これらの製品がイギリス政府ならびに公共セクター御用達であると広告することが許されるのである。

＜英国政府使用のＣＡＰＳ製品（政府御用達製品）リスト＞（参考文書Ｂ20）

製品の種類（等級）	会社名	製品名	製品概要
極秘製品	ZAXUS	SAFEDIAL V1.37	CESG ｱﾙｺﾞﾘｽﾞﾑで稼働する V.34 規格の暗号化された PC-ｶｰﾄﾞﾓﾃﾞﾑ。公開鍵暗号を使用。
極秘製品	ZAXUS	Datacryptor2000 Range	8Mbs で暗号機器に接続。CESG ｱﾙｺﾞﾘｽﾞﾑで稼働。公開鍵を使用。
秘製品	DMS	CASQUE	ｼｽﾃﾑ内部の機微な情報のためのｱｸｾｽｺﾝﾄﾛｰﾙ。
秘製品	ENTEGRITY SOLUTIONS	Secrets For Windows HMG	“ﾄﾞﾗｯｸﾞｱﾝﾄﾞﾄﾞﾛｯﾌﾟ”ﾌｧｲﾙの暗号化。
秘製品	ENTEGRITY SOLUTIONS	Layer7	暗号機能の図書館
秘製品	MARCONI SECURE Systems	DM8000MKIII	ﾊﾝﾄﾞﾍﾙﾄﾞﾗｼﾞｵ。
秘製品	MULTITONE	Z Page	ｱｸｾｽｺﾝﾄﾛｰﾙと暗号化ﾒｯｾｰｼ機能の暗号ﾍﾟｰｼﾞｬｰ。

秘製品	PORTCULLIS COMPUTER SECURITYLtd	Guardian Angel	ｽﾀﾝﾄﾞｱﾛｰﾝ PC のｱｸｾｽｺﾝﾄﾛｰﾙ、起動保護、全ﾌｧｲﾙの暗号化。
秘製品	Reflex Magnetics	Datavalut	ﾊﾞｰﾁｬﾙﾃﾞｨｽｸ暗号を通した基準等級暗号化とﾌｧｲｱｶﾞｰﾄﾞを使用したｱｸｾｽｺﾝﾄﾛｰﾙ。
秘製品	Topsoft	Cyberlock Data	ｺｱｻｲﾊﾞｰﾛｯｸ、ｻｲﾊﾞｰﾛｯｸﾃﾞｰﾀ、ｱｸｾｽ MDL4 を含む PC ｾｷｭﾘﾃｲｽｰﾂ。
秘製品	ZAXUS	Datacryptor 2000 range	8Mbs で暗号機器に接続。CESG ｱﾙｺﾞﾘｽﾞﾑで稼働。
文書ｾｷｭﾘﾃｨと認証	ABATHORN	Abathorn Process	ｺﾗｳﾄﾞｶﾊﾞｰ原理を使用したﾍﾞｱﾗ文書のｾｷｭﾘﾃｲと認証
機密製品	BALTIMORE TECHNOLOGIES	ED600R	X25 ﾘﾝｸ暗号機、64Kbs までﾃｰﾀ速度をｱｯﾌﾟ。
機密製品	BALTIMORE TECHNOLOGIES	ED2048R	2Mb ﾗｲﾝ暗号機；X21、G703、G704
機密製品	BALTIMORE TECHNOLOGIES	ED8000RL	IP 暗号機。
機密製品	BALTIMORE TECHNOLOGIES	NSW/CG600	全ﾎﾞﾙﾁﾓｱﾗﾝﾌﾞ-ﾀﾝ製品と認証と自動鍵配送でﾈｯﾄﾜｰｸ管理をしているに使用できるﾈｯﾄﾜｰｸｾｷｭﾘﾃｲﾜｰｸｽﾃｰｼｮﾝと認証ﾕﾆｯﾄ。
xGSI 認定製品	ENTEGRITY SOLUTIONS	HMG CASM for Exchange	これら製品は安全性免除ﾒｶﾆｽﾞﾑの基本を形成するために結合される。交換の CASM は、原文の証明とｾｷｭﾘﾃｨﾗﾍﾞﾘﾝｸﾞｻｰﾋﾞｽをｻﾎﾟｰﾄする安全なﾒｰﾙｸﾗｲｱﾝﾄである。
xGSI 認定製品	ENTEGRITY SOLUTIONS	Key Server	ｼｽﾃﾑ内部の認証鍵の生成と管理手段を提供する。
xGSI 認定製品	ENTEGRITY SOLUTIONS	Archive Client	後日の法的な監査を考慮し、明確なｱｰｶｲﾌﾞ受け取りのためのﾌﾞﾗｲﾝﾄﾞｺﾋﾟ-の安全なﾒｯｾｰｼﾞのｵﾌﾟｼｮﾝを含む。

ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	COMPAQ	・VMS6.0 ・OPEN VMS6.1 ・OPEN VMS/VAX 6.1 ・SEVMS6.0	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	EDS	ｿﾗﾘｽ 2.6、CESG認可のﾌｧｲｱｶﾞｰﾄﾞﾊﾟｽﾜｰﾄﾞ生成と暗号ｱﾙｺﾞﾘｽﾞﾑで商用ﾊﾟｽﾜｰﾄﾞ暗号ｱﾙｺﾞﾘｽﾞﾑを置き換え。	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	HEWLETT-PACKARD	HP-UX Version10. 20	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	IBM	・AIX V3.0 ・CMW	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	ICL	・VME GSO/GHSO ・DRS/NX ・ISSPO SPARC DRS6000 ・ISSPO INTEL DRS3000 ・ISSPO PC AM250 ・ISSPO PC AM3000	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	COMPAQ-MICROSOFT Partnereship	・Security Enhancements for Microsoft WindowsNT3.51 ・Security Enhancements V1.0 for Microsoft WindowsNT4-	

ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品（続き）	COMPAQ-MICROSOFT Partnereship（続き）	NT（SE）1.0 ・Security Enhancements V1.2 for Microsoft WindowsNT4-NT（SE）1.2 ・Security Enhancements V2.0 for Microsoft WindowsNT4-NT（SE）2.0 ・Security Enhancements V2.1 for Microsoft WindowsNT4-NT（SE）2.1 ・Security Enhancements V3.1 for Microsoft WindowsNT4-NT（SE）3.1 ・Security Enhancements V3.2 for Microsoft WindowsNT4-NT（SE）3.2 ・Security Enhancements V1.0 for Microsoft Windows NT	

ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品（続き）	COMPAQ-MICROSOFT Partnereship（続き）	Terminal Server4.0-WTS（SE）1.0 ・Security Enhancements V1.0 for Microsoft Windows NT Terminal Server4.0-WTS（SE）1.0-1 ・Security Enhancements V1.0 for Microsoft Windows NT Terminal Server4.0-WTS（SE）1.0-2 ・Security Enhancements for Microsoft Windows2000	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	SEQUENT	・DYNIX4.1 ・DYNIX/PTX4.4	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	SUN MICROSYSTEMS	・SOLARIS2.5.1SE ・SOLARIS2.6SE	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	TOPSOFT	Cyberlock Access	
ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品	PORTCULLIS	・DAD（Data Access Defender）-cut down GUARDIAN	

ﾊﾟｽﾜｰﾄﾞ取り扱いﾊﾟｯｹｰｼﾞ（PHP）とｱｸｾｽｺﾝﾄﾛｰﾙ製品（続き）	PORTCULLIS（続き）	ANGEL ・GA NT- GUARDIAN ANGELpassword accesscontrol、NT version ・GA NT 95- GUARDIAN ANGEL password accesscontrol、Windows 95 version ・GA NT 98- GUARDIAN ANGEL password accesscontrol、Windows 98 version ・GA SP - GUARDIAN ANGEL password accesscontrol、Windows 95、98 NT	
暗号評価の製品	BALTIMORE TECHNOLOGIS	ED20M	ED8000IP 暗号機の極秘等級の新世代
暗号評価の製品	COMPAQ	Exchange（SE）	安全なメッセージング、CASM準拠
暗号評価の製品	NETWORK ASSOCIATES	PGP for HMG	基準等級のﾈｯﾄﾜｰｸﾃﾞｰﾀ暗号
暗号評価の製品	PORTCULLIS COMPUTER SECURITY	PENS	ｴﾝﾄﾞﾕｰｻﾞｰ役割をベースとした許可実施ファイルと RSA 鍵管理を備えた基準等級の128ﾋﾞｯﾄ暗号機（ｵﾌﾟｼｮﾝにﾄﾘﾌﾟﾙ DES を含む）

b) UKITSEC 計画

UKITSEC 計画は CESG と貿易産業省による共同管理下に置かれ、CESG 職員をスタッフとする認定機関(CB)により、日々運営されている。コンピュータ・セキュリティへの危険性監視、検査方法と検査技術の保守、個々の評価の監視、これらの評価から得られる安全性レベルの認定が責任範囲であり、CB は欧州基準認定機関の資格を持っている。2000 年 3 月に CB は、イギリス認定局により、共通規準、IT セキュリティ評価規準、およびイギリスシステム・セキュリティ信用度に関する適合認定書を発行する資格を与えられた。

検査は CLEF と呼ばれる第三者組織が行う。CLEF は、厳しい品質およびセキュリティ基準に合格することで、CB が指名する。現在イギリスでは、Admiral, Data Sciences, EDS, Logica, Syntegra の 5 社が CLEF がとして業務を行っている。

1991 年以来、この計画ではテスト基準として EU の IT セキュリティ評価規準(ITSEC)が使われてきた。ITSEC はイギリス、フランス、ドイツ、オランダにより、以前からあるアメリカ規準(注)をもとに開発されたものである。(ITSEC に関する詳しい方法および技術情報については、参考文書B22-B32)

＊(注) 1980 年代に、イギリス、ドイツ、フランス、オランダは、それぞれ国家規準の改定を行った。それらを調整して公表したものが、情報技術セキュリティ評価規準(ITSEC)である。その最新版である 1.2 版は 1991 年 6 月に欧州委員会が発行したものである。その後、1993 年 9 月に、ITSEC 評価を実行する際に従うべき手順を明記した IT セキュリティ評価マニュアル(ITSEM)が発行されている。

UK ITSEC プログラムの最近の活動例として、2001 年の下記の認可があげられる。

- 委任/PKI5.1 からの委任/認可、2001 年 2 月認定決定、EAL3
- 委任/PKI5.1 からの委任/RA、2001 年 2 月認定決定、EAL3
- Cisco Secure PIX Firewall、2001 年 1 月認定決定、EAL4
- Privilege Directed Content Protection Profile(特権指示内容保護プロフィール)、2001 年 1 月認定決定、EAL4
- Check Point VPN-1/Firewall-1 Version 4.1 SP2、2001 年 1 月認定決定、E3
- IBM 遠隔管理センター、2001 年 1 月認定決定、E1

(最新の委任/認可に関するセキュリティ・ターゲット・レポートは参考文書B35)

c)CESG がリストするアドバイザー計画(CLAS)

情報セキュリティ(Infosec)についてすぐれた助言を求める声はますます高まっており、イギリス政府省庁がそれらのネットワークを政府保証イントラネット(GSI)提案に沿うものにしようとしている現在、CESG はさらなる特定助言の要求が出ることを予測している。

CESG 自身はこれらの要望に応えるために、高度の知識と情報に裏打ちされた助言をできる人材を増強する必要に迫られている。

そこで CESG は、イギリス政府省庁に Infosec が認める助言を与える計画である CLAS を開発した。この計画の目的は、イギリス政府省庁および機密公式情報の処理を行うイギリスの機関に Infosec の助言を与えるコンサルタントをプールすることにある。CESG 独自の Infosec 知識を民間セクターの専門家および人材と結び付ける官民のパートナーシップといえる。

この計画の重要な目的は、民間セクターの Infosec 提供者に、公的システムへの危険性、彼らが入手し得る技術、および現行の政府方針とガイダンスを十分に理解させることである。さらに、地方自治体や保健機関のようなイギリス公共セクターが、政府の標準 Infosec の助言を得やすくすることも目指している。

CLAS は CESG により管理と監視が行われ、CESG はアドバイザーの資格に関する基準を明確化している。この計画には民間セクターのコンサルタントの情報と訓練プログラムが用意されており、希望者は基準に合格するか、適切な訓練コースを終了するかのいずれか、または両方の条件で「CESG 認可」の資格を与えられる。

資格要件と会員条件を満たすものは誰でもこの計画の参加会員になることができる。大手の IT 企業も、小さなコンサルタント会社も等しく参画できるのである。費用は会費制で賄われる。

d)IT ヘルス・チェック・サービス(CHECK)

IT ヘルス・チェック・サービス、すなわち CHECK は、CESG が認可した民間セクターの企業が IT ヘルス・チェック・サービスを政府機関に対して行えるようにすることを目的にしている。CHECK は、CESG と防衛評価研究局(DERA)とが共同制作したガイドラインを使って、無防備な点の検査を行い、ネットワークやシステムの IT セキュリティー上の弱点を検知できる。

CHECK は、1999 年 4 月に始まった試験期間を経て 1999 年 10 月 1 日に発足した。CHECK は、公知の弱点や共通の構造上の欠陥を利用した多数の検査でシステムやネットワークの危険個所を検出するサービスである。検査結果は、危険個所の詳細とセキュリティ上の有効対策提示を盛り込んだレポートの形で依頼者に通知される。

イギリス政府では、伝統的に CESG や DERA から選ばれた専門家チームがこれらのサービスを提供してきた。その結果、両機関は高い評価を受けている。CESG と DERA は、今後も、通常の秘密または高レベル機密データへの特別なヘルス・チェックを提供し続けるだろう。

政府保証のイントラネット(GSI)や他の政府主導 IT の立ち上げに伴い、イギリス政府省庁の IT ヘルス・チェック機能に対する需要はかなり増大した。CESG や DERA は、危機管理国家インフラストラクチャ(CNI)イニシアティブに関連する政策や必要条件の出現にともない、その需要が更に増すと予想している。

CHECK は、この拡大する需要に対処するため、CESG と DERA の知識を民間セクターが活用できようにすることを意図したものである。

CHECK の主要目標を次のとおりである。

- イギリス政府政策に沿った IT ヘルス・チェック・サービスが提供できるようにする。
- Infosec 基準 No.1(Memo 10)に沿ったヘルス・チェック保証をイギリス政府の最低要件を満たすものにする。
- 現在、民間セクターの会社が提供している IT ヘルス・チェック・サービスを強化する。
- 依頼者のニーズ変化に迅速に対応できる融通性のあるサービスにする。
- 危機に対する国家インフラストラクチャに関する政府方針の結果として予想される需要に備える。

(4) CESG 認可および ITSEC 認定製品リスト

現在 CESG は、評価を受けたか、または認可された製品とシステムのリストを 2 冊に分けて発行している。「CESG 認可製品計画(CAPS)製品リスト」と「イギリス IT 認定計画認定製品リスト」である。

しかし、CESG はこれらのリストを、「CESG 認可および認定製品リスト」としてまとめる作業を行っており、新しい「CESG 認可および認定製品リスト」は年刊で、2 月から 3 月に印刷され、同時に CESG ウェブサイトに掲載される。このウェブページは、必要があれば年間を通してかなりの回数で更新される。

(5) その他の CESG プログラムおよび政府が使用する製品

- CLOUD COVER:試験的公共基幹インフラストラクチャ(PKI)を開発して、イギリス政府省庁間の通信(電子メール、ファイル転送、電子商取引など)をサポートするプログラム。
- KILGETTY:PC に保存されたイギリス政府のデータを保護するための CESG が企画した製品グループ。
- THAMER:イギリス政府が使用する CESG の新世代データ・リンク暗号化法。THAMER は最高機密レベルまでのデータを保護できる。固定ポイント・トゥ・ポイント同期通信リンク全体にわたり、データ転送速度 2.048 メガビット/秒で実行される。ユーザーが必要なシステム構成を選択できるようにインターフェース・モジュールのセットが提供される。
- BEDERAL: BEDERAL は高性能暗号装置で、イギリス政府が使用する目的で CESG が開発した。
- CATAPAN: CATAPAN(BID/1550)は ATM ネットワーク用の高性能暗号装置である。事務所のデスクトップ用に、または PC ラックに置くようにデザインされており、頑丈な装置である。
- HANNIBAL: HANNIBAL は ISDN で使う安全な電話で、EURO ISDN 上で極秘レベルまでの音声とデータを保護できる。

- EUGENIC: EUGENIC は、CESG が設計した、独立型、汎用、暗号装置で、安全なポイント・トゥ・ポイント通信回路の端末に取り付ける。この装置はデータ転送速度範囲 1.2 キロビット/秒から 10 メガビット/秒までの、同期デュプレックス V10/V11 ラインを使う通信を保護する。
- PRITCHELⅡ: PRITCHELⅡは CESG が設計し保証した暗号標準カーネルで、イギリス政府および他の認可を受けた取引先への販売を意図したセキュリティ装置に組み込まれる。すべての機密保護マーク付き情報のデータ暗号化および復号化について認定されており、アメリカおよび NATO の次世代保護装置の暗号との互換性を持つ。
- RAMBUTANⅡ: RAMBUTANⅡは CESG が設計し保証した、暗号標準カーネルで、イギリス政府および他の認可を受けた取引先への販売を意図したセキュリティ装置に組み込まれる。
- CASM 安全メッセージング・パンフレット:今では CESG から入手できない。CASM は政府の省庁に、その電子メールシステムの安全性についてアドバイスとソリューションを提供する CESG プログラムである。CASM は、安全な e-メールのためのアーキテクチャ、アーキテクチャを明記した完全な文書のセット、アーキテクチャをサポートする製品のセット、工業界に対する商品開発のための助言と援助、政府に対するアーキテクチャを正しく実装させるための助言と援助、および技術のデモを提供する。
- SHELLEYAN: SHELLEYAN は CESG がイギリス政府のために開発した高性能暗号装置である。

第４章　フランスの電子署名関連の法律および規則

フランス法は暗号装置を 2 つのカテゴリーに分けていた。一方は、暗号(例えば電子署名)により通信の認証または安全性のみを有する装置であり、もう 1 つのカテゴリーには、他のすべての暗号テクノロジー(例えばメッセージやファイルの暗号化に関するもの)が分類される。このカテゴリーによって、政府への手続が若干異なっていた。たとえば、以前は、認証や安全性のための暗号(例えば電子署名)の使用においては、フランス中央情報システム安全局(DCSSI)への申告書の提出が必要であった。実際には、フランス国内での認証用装置の供給と使用は慣例として許可されていた。1996 年、にフランスは認証/安全性暗号に関する規制をやや緩和する新しい法案を可決した。この法律では、機密性を与えない暗号は規制を受けずに使用できる(すなわち前もって申告する必要がない)。

2000 年 2 月 29 日、EC 命令を採択する法案が可決され、2000 年 3 月にこの法律が施行され、暗号技術の改正を含む新法となった。

本章では下記項目を報告する。

１．　電子署名に関する最近の法律および規則

２．　電子署名関連の法律と規則に対する産業界の反応

１．電子署名に関する最近の法律および規則

1999 年から 2000 年にかけて、フランス政府は暗号の使用に対する厳しい政策を緩和する数多くの新しい法律および規則を制定した。

(1) 1999 年から 2000 年　自由化政策の策定

1999 年 1 月暗号技術の国内使用が自由化された。1999 年 1 月 19 日の、情報化社会に関する内閣委員会で、フランス政府は「商品取引とプライバシー保護に関する法律の枠組構築」と題する文書の中で暗号技術政策について下記のような変更を発表した。

暗号：フランス国内での全面的自由化

- 暗号製品の使用を、ワッセナーアレンジメント合意の鍵長 56 ビット超暗号輸出規制だけを残し、全面的に自由化する。
- 暗号キーを信頼できる第三者に預託しなければならないという強制性をなくす。第三者の役割をキーの管理だけに限定せず、電子署名の認証のような他のタスクまで拡大できる。そのような装置への預託および自動預託メカニズム導入を促進する。信頼できる第三者は公開で当局に認定の申し込みができる。
- 違法な結果をもたらす暗号技術の使用を当局が効果的に取り締まることができるようにする。違法な使用については、当局が要求する場合は暗号化した文書の解読コピーを提

出することを義務付け、罰則を設けて現行の法律を補足することで対処する。さらに、当局側の技術的能力を相当程度強化する。

(2) 電子文書および電子署名：法的障害の除去

・欧州連合の方向へ一致させる。

・すべての必要な保証とともに電子文書および電子署名の証明機能を配慮する。

ジョスパン首相が暗号の国内規制を自由化すると表明（参考文書B41・B42）した。この緩和で TTP へのキー預託の強制性がなくなり、フランス政府は、取り締まり当局の要請があれば、暗号化文書の平文テキストを裁判所に提出させることができるようにした。こうした政策の変化は、規制政策が国内の電子商取引の成長を阻害しているとの認識が政府内で高まった結果生じたものである。彼はまた「政府側の怠慢」を含む多くの障害があることも認め、政府は電子商取引を支援する方向で政策の調整を行っていると強調した。

最後に、2000 年 2 月、「証拠構成法ならびに電子署名」（参考文書B47）法案と呼ばれる電子署名に関する新法が導入された。この法案は 2000 年 2 月 29 日に議会を通過した。この法令は情報技術を考慮に入れ、電子文書および電子署名の法的効力を認めることで、証拠に関するフランス法を変えた。この法令により E-署名に関する EC 指令をフランス法中に取り入れることも実現した。

この法令は、1999 年 8 月に首相が表明した法令プログラムの第一歩である。このプログラムは、個人データの保護に関する法案の提出、そしてさらに 2000 年後半のフランスが情報化社会に入るのを加速するのに必要な多くの法規の一括提出へとつながっていった。

２．電子署名関連の法律と規則に対する産業界の反応

フランス産業界は暗号規則に関しては政府の厳しい管理下におかれていた。暗号技術の使用に関するフランスの規則は、1990 年代の大半を通じて、世界一厳しいものに数えられた。しかしながら

・ フランス産業界は、この国の電子商取引の成長を阻んでいるのはこの規制そのものだとして、その緩和を求める強力なロビー活動を行った。

・ 1990 年代末までに、産業界は政府に、暗号化規制を緩め、逆に支援する方向の政策が必要だという認識を持たせた。

結果、電子署名を含むすべての暗号技術に関する新法が具体化された。

総じて言えば、フランス産業界は電子署名に関する現在の政府方針を支持している。フランスの政策は、現在、基本的には電子署名に関する EC 指令に沿っている。このことは、フランスの大手 IT 企業であるブルが欧州共同体電子署名標準化構想 (EESSI)で主導的活動を行っていることでもわかるように、フランス産業界の利益と一致している。

第５章　フランスの評価機関

本章では、フランスの暗号評価（Encryption　Assesment）に関わる２機関の情報を提供する。

１．　国防総事務局

２．　Direction Centrale de la Securite des Systemes d'Information（情報システムセキュリティ中央局）

国防総事務局とは、首相を直接サポートする局である。事務局は情報セキュリティも含め、広範囲の国防問題に関して首相へアドバイスや助言を行う役割を担っている。

事務局の権限下にある機関の一つが Direction Centrale de la Securite des Systemes d'Information（DCSSI）である。この機関は、以前は Service Centrale de la Securite des Systemes d'Information として知られ、今も頭文字をとって SCSSI の名称で認知されている。SCSSI は、暗号化技術の評価と認証など、情報セキュリティ分野でのフランス政府の活動に責任を負う。

ただし、政府の暗号評価に関しては、公開されておらず、行っているものと推定されるだけである。一般的な暗号製品の認証や評価に関しては公開されている。

１．　国防総事務局（ＳＧＤＮ）

フランス政府の体制の中では、権力は国家の長としての大統領と、政府の長としての首相との間でほぼ均等に分配されている。フランスの首相は（外務省、国防省、内務省、法務省などの）内閣のメンバーを監督するとともに、政府内の各機関間の協調をサポートする多数の「省庁間」機関をも監督する。こうした省庁間機関に国防総事務局が含まれる。

（1）　責務

国防総事務局（SGDN）は、情報セキュリティも含め、広範囲の国防問題に関して首相へアドバイスや助言を行う。SGDN は 1978 年 1 月に設立され、1998 年以降 M.Jean-Claude Mallet が長官の座に着いている。SGDN は以下の権限を有する。

- 防衛問題に関連する政策準備において首相を援助する。
- 危機状態に際しフランス軍の戦闘関する政府委員会の政策を作成する。
- Inter-ministerial Committee for Information Systems（情報システムセキュリティに関する省庁間委員会）（CISSI）を統轄する。
- 機密情報と国防機密を保護する。

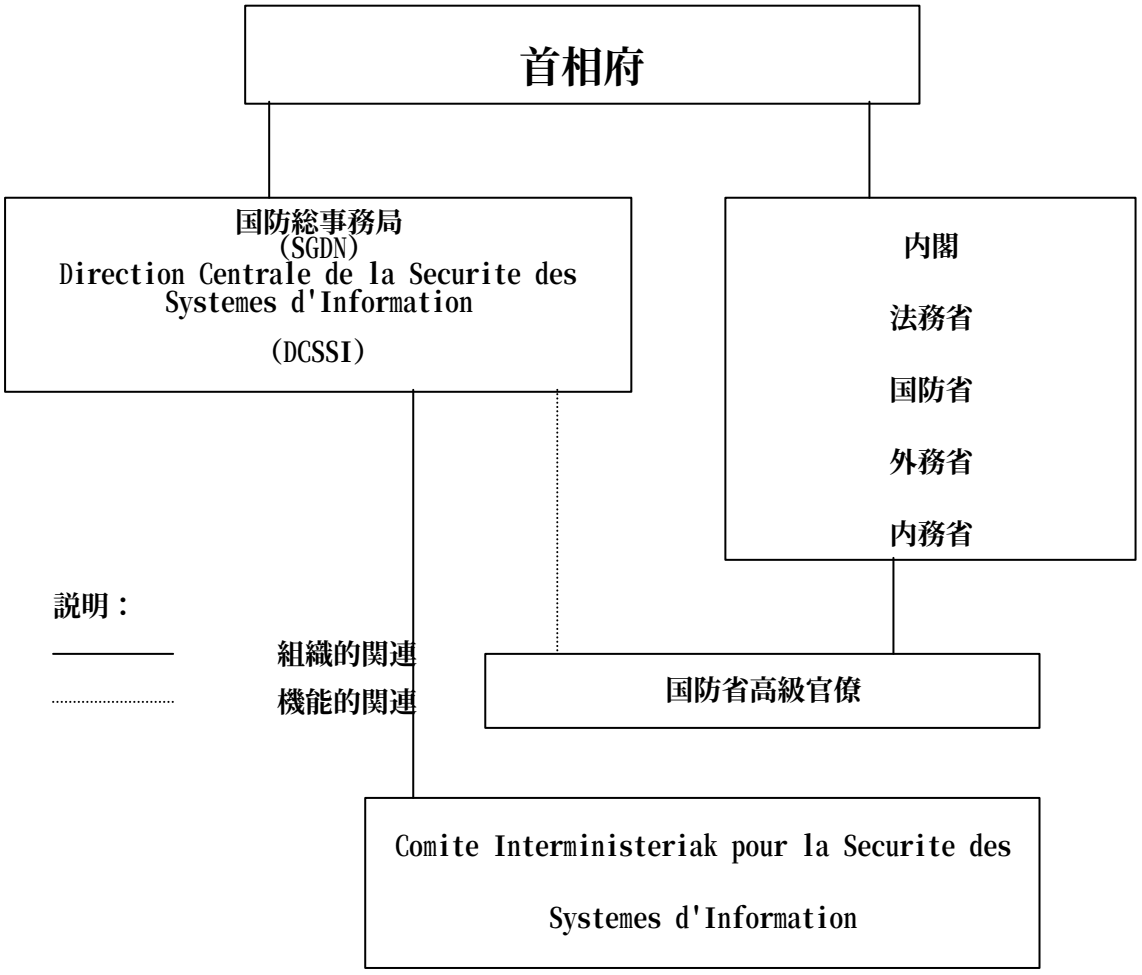
SGDN は、フランス政府の情報セキュリティ政策およびその活動の中心である。この役割に当たり、SGDN は Direction Centrale de la Securite des Systemes d'Information（DCSSI）、もしくは通称 Service Centrale de la Securite des Systemes d'Information（SCSSI）を監督する官庁である。DCSSI は情報セキュリティ分野でのフランス政府の活動に責任を負い、具体的には暗号化技術の評価と認証などの分野の SGDN の政策を実行する。

（2）IT 関連機関の構成

SGDN のスタッフは以下の 6 部門から成る。

- Comite Interministriel du Renseignement（情報に関する省庁間委員会）
- Direction des Affaires Internationales et Strategiques（国際紛争・戦略局）
- Direction de la Protection et de la Securite de l'Etat（国家セキュリティ保護局）
- Direction des Technologies et Transferts Sensibles
- Direction Centrale de la Securite et des Systemes d'Information (DCSSI)
- Direction de l'Administration Generale（統轄管理局）

DCSSI は、IT 分野での SGDN の活動に責任を負う。SGDN は 1996 年に SCSSI の監督官庁となった。次の図表は、首相が SGDN、DCSSI、Inter-ministerial Committee for Information Sytems（CISSI）の上に立つという「命令系統」を示している。



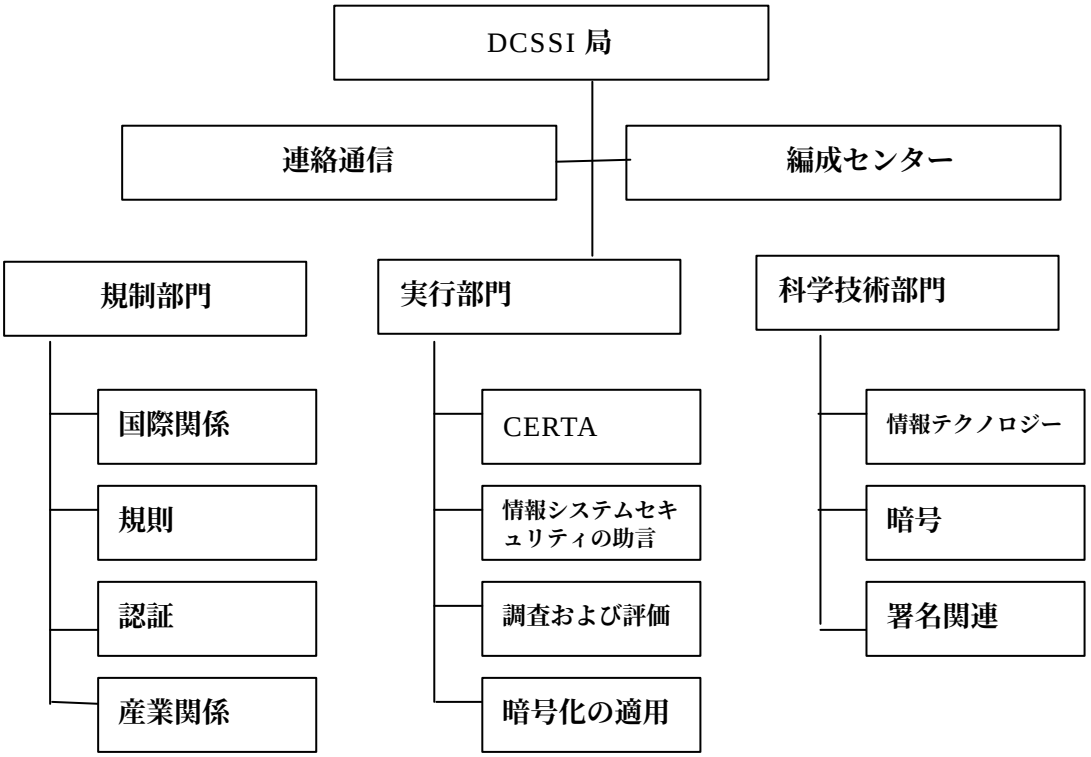
２．Direction Centrale de la Securite des Systemes d'Information（DCSSI）

Direction Centrale de la Securite des Systemes d'Information（DCSSI）は、フランス政府の情報セキュリティ政策およびその実行において、フランスのその他の諸機関を支援する。2000 年 4 月より、DHERRI SERRES 氏がディレクターをつとめており、コンピュータ・セキュリティの開発者を新たに雇用し、暗号の分析および復号に対する脅威に対する体制を強化している。

（1） 組織の構成

DCSSI は以下の 3 つの主要部門から成る。

- 規制部門：この部門は DCSSI の産業関係と国際関係を担当する。同部門は、情報セキュリティ分野での DCSSI の規則を作成し実施する。また、認証業務も行う。
- 実行部門：この部門は、通信および情報セキュリティの分野でのフランス政府の施行をサポートする。同部門は CERTA プログラムを実行し（下記参照）、情報テクノロジー分野において他の政府諸機関をサポートし、政府の情報セキュリティシステムを調査および評価し、政府機関内部での暗号化の使用を監督する。
- 科学技術部門：この部門は情報テクノロジー、通信セキュリティ、暗号化の分野で、フランス政府を代表して DCSSI の実行を技術的にサポートする。



DCSSI の主要責務の一つに CERTA プログラムがある。CERTA は 1999 年に SGDN によって制定され、1999 年 10 月以降実施されている。DCSSI の下、CERTA は、コンピュータのセキュリティの問題に対処するフランス政府のために、不正な攻撃の可能性を弱め、諸機関のセキュリティの直接コストを減少させ、間接的損害のリスクを軽減することが役割である。

CERTA は報告されたセキュリティ事故を全て記録、照合、分析する。CERTA はサイト管理者やセキュリティ問題に従事する専門家間の連絡を簡易化するため、その他のフランス政府諸機関と緊密に協力し合う。また、システムの脆弱性、国防戦略および防衛機構、政府全体に対し起こりうる攻撃の早期警告など、セキュリティ情報のチェックとその結果の配布も行う。

CERTA は許可を特別に得ない限りは、送られてくる情報の機密を保持する。CERTA は日常的なネットワークやコンピュータの管理は行わず、むしろ、他機関の政府情報担当官にアドバイスを提供する。

(2) 実行方法：認証とプロフィール

評価／査定の分野で、DCSSI は暗号製品を評価する認証プロフィール（すなわち規格）を多数作成してきた。(DCSSI の評価および認証手続きに関しては、参考文書B48)

これらのプロフィールを下記の表にリストアップする。(実際のプロフィールおよび政府の認証の写しも参考文書B48)

DCSSI の暗号製品の評価／認証プログラムは、欧州 ITSEC および共通基準に統一させている。(参考文書B49 では、ITSEC と共通基準プログラムに基づく相互認知に関する DCSSI の陳述書を示す。)

プロフィール	産業パートナー	証明書	プロフィール
Smart Card IC with multi-Application Secure Platform	Eurosmart	参考文書B50	参考文書B51
Transactional Smartcard Reader	Cyber-COMM	参考文書B52	参考文書B53
Smart Card Integrated Circuit with Embedded Software	Eurosmart	参考文書B54	参考文書B55
Intersector Electronic Purse and Purchase Device	GIE Cartes Bancaires CB Societe Financiere du PMEI	参考文書B56	参考文書B57
Intersector Electronic Purse and Purchase Device	GIE Carters Bancaires CB	参考文書B58	参考文書B59

(Version of Pilot Schemes)	Societe Financiere du PMEI		
AutomaticCash Dispensers/Teller Machines	Bull Dassault AT Diebold NCR Siemens Nixdorf Wang Global	参考文書B60	参考文書B61
Configurable Security Guard (CSG)	Delegation Generale pour l'Armement	参考文書B62	証明書のみ
Firewalls V2.2	Delegation Generale pour l'Armement	参考文書B63	参考文書B64
Firewalls V2.2	Delegation Generale pour l'Armement	参考文書B65	参考文書B66
Carte a puce Billettique Avec et Sans Contact	RATP SNCF	参考文書B67	証明書のみ
Smartcard Embedded Software	Schlumberger	参考文書B68	参考文書B69
Smartcard Integrated Circuit Protection File	Motorola Phillips Siemens AG STMicroelectronics Texas-Instruments	参考文書B70	参考文書B71

SCSSI の暗号製品の評価および認証は、認可された Centres d'Evalution de la Securite des Technologies de l'Information（情報技術セキュリティ評価センター）（CESTI）によって実行される。現行および懸案中の CESTI には、AQL、CEACI（CNES-SOREP）SERMA-Technologies、ALGORIEL、CEA-LETI、ES2 がある。

(3) 最近の活動：製品の認証

上記にリストアップした基準およびプロフィールに基づき、DCSSI はいくつかの暗号製品を認証したが、認証はフランス政府による製品の推奨を意味するものではないと DCSSI は極めて入念に強調している。さらに、いかなる DCSSI の認証も、評価された製品の特定バージョンにのみ適用されるのであり、新しいバージョンはまた独自の認証を得なければならない。

認証とともに、DCSSI は認証報告書を作成する。各報告書には、評価の主要な結論が提示

される。これらの報告書はASCSSIによりインターネットに掲示され一般に入手可能である。

2001年、SCSSIは以下の製品に対し新たな証明書を発行した。

・ Oberthur Card Systems、Gemplus および Trusted Logic/Groupement Carte Bleue 社提供のアプリケーション、Oberthur B0' v1.0.1 et GemClub v1.3 chargees sur la plate-forme Javacard/VOP GemXpresso 211 V2。（参考文書B73）

・ ATMEL Smart Card および Ics/ATMEL Smart Card Ics.社提供のマイクロサーキット、ATMEL AT05SC3208R（AT55898 rev.Q に準拠）。（参考文書B74）

・ Infineon Technologies AG/Credit Mutuel 社提供のマイクロサーキット、SLE66CX160M（M1401C13 に準拠）。（参考文書B75）

第６章　ドイツの電子署名関連の法律および規則

電子署名に関する現行のドイツの法律および規則の基礎は、1997 年のデジタル署名法である。デジタル署名法は技術に関する法律で、デジタル署名の法的妥当性は扱っていない。むしろ、デジタル署名法は、ドイツでのデジタル署名利用に向け、安全なインフラの条件を提供することを目的としている。法律の遵守は「任意」だが、法律が可決された際にドイツ政府は、政府のセキュリティ機関である情報技術安全局（ＢＳＩ）が、デジタル署名使用の事実上の基準作成する意図を明らかにした。

2000 年 9 月、ドイツ連邦政府内閣は、デジタル署名法の改正を承認した。法律改正は以下の 2 組の立法から成る。

・ デジタル署名法の修正、および
・ 民法と民事訴訟法の修正、これにより電子署名の法的地位が強化される。

改正案は現行法の実質的変更を示している。電子署名に関する EC 指令の要件をドイツ法に組み込むとともに、同法で使用される構成や用語も実質的に変更する。認証機関の自主認定スキームに加え、認定済み認証機関の利用の実質的インセンティブも導入される。同時に、修正はデジタル署名法の基本概念、すなわち、政府機関監督下の PKI（公開鍵基盤）技術に基づく、電子署名の自主的な安全性の高いインフラという概念は維持されている。

本章では、下記項目に関して報告する。

１．電子署名関連の最近の法律および規則
２．電子署名関連の法律と規則に対する産業界の反応

１．電子署名関連の最近の法律および規則

(1)1997 年 6 月　ドイツデジタル署名法（「マルチメディア法」の第 3 条）議会（Bundestag）可決

デジタル署名法は「技術的な」法律で、デジタル署名利用に向け安全なインフラの条件を提供することを目的としており、法的妥当性を規定はしていない。法律の遵守は「任意」だが、法律が可決された際にドイツ政府は、デジタル署名使用の事実上の基準を作成する意図を明らかにした。このため、ドイツの産業界は、アメリカの国家安全保障局に相当するドイツの BSI が、同法に基づく技術規格の設定に深く関与することに関心を抱いた。BSI は産業上の問題ではなく、セキュリティの問題を中心に扱う。したがって、同法からはドイツのデジタル署名使用に関する競争的な市場主導による手続は生まれないだろうという懸念があった。

(2)1997 年7月　ドイツデジタル署名条例の発表

デジタル署名法の実行指針が規定されたドイツデジタル署名条例が 1997 年 7 月に発表され、11 月署名条例（参考文書B80）を完成させた。条例では、認証機関の要件および責任と、デジタル署名の作成に使用される技術コンポーネントの最終要件が規定された。

（3）1997 年 11 月　BSI による技術カタログ案（Mabnahmenkataloge）の発表

これらのカタログでは、認証機関に対するデジタル署名法および条例に基づく指導とデジタル署名の手続が記述された。公聴会が開かれたが、BSI の熱心な作業を賞賛しつつも、産業界の代表はカタログに関し以下のコメントを挙げた。

1) 長さ（トータル 300 頁以上）と複雑さ故に、理解と実行が難しい。
2) 不要な多くの分野を規定している。多くの業界代表者は、カタログの第 5 および 6 項のみがデジタル署名条例に基づき実際に必要であると指摘した。
3) 規範的な言い回しでありながら、同法および条例を満足する技術的尺度を単に例示しているだけである。
4) 現行フォームでは柔軟性に欠け、特定基準のデジタル署名の使用に限定されがちとなる。
5) カタログは国際的な基準や発展とは相容れない。
6) ITSEC E4 "high"レベルの使用は、デジタル署名の利用の多くにとって過度である。

技術カタログ案のコメントは、ドイツ政府のデジタル署名政策を緩和するうえで、ドイツ産業界にとって重要な功績だった。

(4)1998 年 2 月　技術証明書の認証企業の公表

ドイツ政府はデジタル署名法およびデジタル署名条例に基づく技術コンポーネントとセキュリティ・プランの認証を行う政府が認可した会社を公表した。

ＢＳＩだけでなく、民間企業として最初に Telesec（ドイツテレコム社）と SignTrust（ドイツポスト社）も認可された。認可された認証機関の発行する証明書を使用することで、デジタル署名はデジタル署名法に基づく法的地位が得られる。1998 年 9 月以来、マインツの Telecommunications & Post 認証機関（CA）（国内最上位認証機関）が業務を開始している。

(5)1998 年 8 月　デジタル署名の国際的承認に関するドイツの政策

ドイツ政府は、デジタル署名の国際的承認に関する政策方針書を公表したが、業界のアナリストの意見では、相互認知に関する政府の考えが非現実的で、他の国も全て（ドイツデジタル署名法の下でのような）中央最上位認証機関（ルート CA）を備え、登録機関を中央集権化すると想定しており、デジタル署名の国際的承認を後退させる内容であった。

(6)1999 年 6 月「ドイツ暗号政策のコーナーポイント」の発表

「ドイツ暗号政策のコーナーポイント」(Eckpunkt de deutschen Kryptopolitik) を発表し以下の 5 点の基本指針が述べられている。

1) 政府は暗号の自由な利用を制限する意図はない。
2) 政府は安全な暗号の信託機構を確立する手段を講じる。
3) 政府は、安全かつ高性能な暗号製品を開発できる暗号メーカーの能力を必須と考える。
4) 強力な暗号の普及によって、政府の傍受能力が損なわれてはならない。したがって、発展は注意深く監視する必要があり、2 年後には報告書が発行される。さらに、政府は法執行機関およびセキュリティ機関の技術的能力を向上させる。
5) 政府は暗号政策の国際協調を大いに重視する。政府は、市場主導型の開放的な基準と共同利用システムとを主張する。

この初めて明確になった政府声明は、暗号の流通と使用制限に強力に反対する立場にとって意義深く、重要である。欧州では（フランスとイギリスでの自由化に続き）暗号の制限に反対する趨勢が続くことになった。ドイツの暗号分野の競争力強化や、暗号製品の政府による自発的な認可の強化なども重要な意味を持つ。

(7)2000 年4 月　電子署名の体制確立法（署名法）－法案のキーポイント（参考文書B85）

電子署名に関するＥＣの命令の実行に必要な活動の設定をした。

同年 8 月、デジタル署名法の修正（参考文書B86）を承認し、9 月には民法と民事訴訟法の修正案により、電子署名の法的地位が強化された。(参考文書B87) 11 月に、「電子署名および手数料のユーロへの変更に関する条例作成」(参考文書B88) についての研究報告書を発表した。

(8)2001 年 4 月　電子署名および追加法的要件の修正条件の修正

1)電子署名に関する EC 指令の要件をドイツ法に盛り込み、2) 同法で使用される構成および用語を実質上変更することとなった。

認証サービス・プロバイダー（CSP）の自発的認可スキームは、認可済み認証サービス・プロバイダー利用の実質的インセンティブ（たとえば、国外の証明書でも「同等のセキュリティ」を実証していれば、公認証明書として同等の法的効果を有する）を含めて導入される。同時に、修正案では、デジタル署名法の基本概念、すなわち、政府機関監督下の公開鍵基盤（PKI）技術に基づく、電子署名の安全性の高いインフラ概念は維持されている。この修正案に対する政府の公式コメントがある（参考文書B89）

２． デジタル署名関連の法律と規則に対する産業界の反応

全般的にドイツ産業界は、暗号の厳しい管理に表立って反対の意を唱えた。国際商工会議所ドイツ支部は、暗号に関する政府のイニシアティブと産業界との協調を図ったが、その報告書が示すように、ドイツのビジネス社会は、全般的に暗号規制に反対し、この分野での不要な規制を避けたがっているようである。

（1） ドイツ産業界、デジタル署名規制の緩和を主張

ドイツ産業界は BSI 技術規格が中心となるデジタル署名法では、ドイツでのデジタル署名の利用は、競争性のある市場主導型のものにはならないであろうとその施行に懸念を示し、政府政策の緩和に成功を収めてきた。

- 産業界はデジタル署名条例の BSI 技術カタログ施行阻止に成功した。
- 1998 年に BSI 以外の機関による認可を認めさせた。

現在ドイツ産業界は立法化を前に、審議中のデジタル署名法の新修正案通過を待っているところである。

（2） ドイツ消費者団体、デジタル署名規制を懸念

いくつかのドイツ消費者団体は、使用の違いによりセキュリティ条件が異なる事実にもかかわらず、デジタル署名の全ての利用に同一安全基準を課すという政府の基本方針を支持した。産業界と消費者間の対立は、EU のデジタル署名基準案をドイツ消費者協会が批判していることを例示している。

1998 年 4 月、ドイツ消費者協会は、EU 委員会の電子署名に関する指令案を批判する陳述書を提出した。ドイツ法の厳格な「文書条件」のため、ドイツの消費者保護団体らは、全てのタイプの「電子署名」に法的承認を拡大することに反対した。彼らはむしろ、このような法的承認は、文書による署名と同等のセキュリティレベルに対応する非対称暗号を用いるデジタル署名に限定すべきだと考えた。

この批判は、ドイツ以外の国の低レベルセキュリティ電子署名やデジタル署名によって、ドイツデジタル署名法における高い技術基準が低下してはならないというドイツ人の一般的な見解を反映している。

さらに、この批判は、当事者の意思表明として電子署名を法的に承認したいとするイギリスおよびアメリカと、署名のその他の機能、たとえば法的拘束力を有する取引を始めようとしている当事者に警告する役割を重要視するドイツ法との間にあるギャップを示していたが、現在ではこのギャップは埋まっているものと考える。

第７章　ドイツの評価機関

本章では、以下の機関について報告する。

１．Bundesamt fur Sicherheit in der Informationstechnik（BSI）[連邦情報技術安全局]

２．Bundesministerium fur Wirtschaft und Technologie（BMWi）[連邦経済省]、

３．Bundesausfuhramt（BAFA）[連邦輸出局]。

BSI は IT セキュリティのためのドイツ政府の主要機関である。主な任務は、政府諸機関の IT セキュリティをサポートすることであるが、IT 商業製品の認証業務も行っている。

BMWi はデジタル署名関連の法律や規則の作成および発行を監督する機関であり、具体的には、郵政事業管理局が執行している。

BAFA はドイツの主要な輸出認可機関で、ドイツ暗号製品の輸出に責任を負うが、ドイツ政府あるいはドイツ民間セクターで使用される暗号製品の性能や技術基準面での認可や評価は行わない。

１．Bundesamt fur Sicherheit in der Informationstechnik（BSI）

Bundesamt fur Sicherheit in der Informationstechnik（BSI)、すなわち連邦情報技術安全局は、IT および暗号分野でのドイツ政府の中心機関である。IT システムのセキュリティ維持に際し、ドイツ政府をサポートすることを主要任務とし、ドイツの CERT プログラムをサポートしている。

また、BSI は 2 つの主要分野－、電子署名（郵政事業管理局のサポートを受ける）とセキュリティ製品－での商業製品の評価と認証を行う。

（1）　組織

BSI の現行体制は 1997 年以降に固まった。BSI は Bundesministreium des Innern（BMI)、すなわち連邦内務省の管轄下にある。

BSI は次の 6 つの支局を有し、局長は Dirk Henze 博士である。

① IT セキュリティに関する政府協議：政府内での IT セキュリティ政策の作成と実行を支援する。BSI の副局長がこの支局の統轄にあたる。この支局は政府機関のみをサポートし、民間セクターの支援は行わない。

② 暗号技術：政府が使用する暗号の研究開発を担当する。政府にのみ報告し、民間セクターの支援は行わない。

③ 政府 COMSEC（通信セキュリティ）：政府の通信セキュリティ対策と民間セクターをサポートする。

④ インターネット・セキュリティと共通基準：政府 BSI の IT セキュリティ政策と民間セクターをサポートする。
⑤ 認証と評価：BSI のセキュリティ製品の評価と認証をサポートする。
⑥ デジタル署名局：デジタル署名に関する政策と規則の分野でドイツ政府をサポートする、つまり郵政事業管理局をサポートする。

BSI は情報社会に関連する EC 指令のドイツでの履行にも責任を負い、ITSEC（情報安全評価基準)、EU-CEN（欧州連合標準化委員会)、ETSI（欧州電気通信標準化機構）に参加して、欧州規格の開発プロセスに貢献する。BSI はいくつかの異なるプログラム部門から成る。BSI 下の主要プログラムには、以下が含まれている。

- IT 製品認証
- ウィルス防止プログラム
- 安全な E メールプログラム（スフィンクス・プログラム）
- デジタル署名プログラム

BSI はインターネット・セキュリティの問題、「スフィンクス」プロジェクトでの e メールセキュリティ、e メールの出所を点検する予備プロジェクト「メール・トラスト」など広範囲な分野に関わっている。その他の活動としては、ウィルス識別、警告、いたずらメールの摘発、ファイアウォール（LAN とインターネットの間に置く保安用システム)、修復などがある。デジタル署名プログラムに関しては、認証と承認を管理している（次節で取り上げる）BMWi（連邦経済省）をサポートしている。

（2）実行手段：暗号とセキュリティの評価と認証

イギリスおよびフランスと同様、ドイツもインターネット・セキュリティと共通基準(CC)プログラムに参加している。BSI は多国間および二国間協定に基づき、他国の認証機関による ITSEC と CC 証明書を承認している。ITSEC 証明書の相互承認協定は、1998 年 3 月に発効となった。1998 年 10 月、ドイツは欧州パートナーおよびアメリカ、カナダと共通基準を締結した。

また、ITSEC および共通基準に基づくプロフィールを承認するだけでなく、国内申請通知および解説（AIS:Application Note and Interpretation of the Scheme）も発行している。

2000 年 12 月から発効している「BSI 認証：開発者および流通業者のための情報」（この文書は、認証を取得する技術的および行政的側面と、認証プロセス自体の技術的側面からの情報を提供している）の内容は次のとおり。

- 認証の技術要件（検査を含む）
- 認証の組織要件（コスト、証明書の発行、認証報告書を含む）
- ドイツで使用される ITSEC のセキュリティ基準

・ドイツで使用される共通基準のセキュリティ基準

BSI は認証自体を行うが、製品の技術的評価は通常、BSI によって認可され許可された評価機関（ITSEF－IT セキュリティ評価施設）が行っている。現行の BSI 評価施設には以下が含まれる。

- Industrieanlagen-Betriebsgesellschaft mbH
- Tele-Consulting GmbH
- Debis Syetemhaus Information Security Services GmbH
- TUV Informationstechnik GmbH
- Competence Center Informatik GmbH
- Deutsches Forschungszentrum fur kunstliche Intelligenz GmbH

認証プロセスは、申込者が「BSI による証明書発行申請書」と呼ばれる初期書類を提出することから始まる。（参考文書B97）

（3） 最近の活動

「ドイツ IT セキュリティ証明書：IT 製品および IT システムのセキュリティ」という表題の BSI 報告書が発行されている。この報告書で、BSI に認証された IT 製品の広範なリストを提供している。リストには、他国で発行され BSI に承認された証明書付の製品も含まれる。

各認証プロセスにおいて、BSI は認証報告書を作成する。この認証報告書は公的文書で、BSI または ITSEF のウィザーから入手可能である。

- fun communications GmbH の Transport/S-2.0 に関する認証報告書（参考文書B102）
- IBM Corporation の IBM 2/390 CMOS Computer System Family 用 Processor Resource/Systems Manager(PR/SM)に関する認証報告書（参考文書B103）
- Philips Semiconductors の Philips Smart Card Controller に関する認証報告書（参考文書B104）

2. Bundesministerium fur Wirtshaft und Technologie (BMWi)

Bundesministerium fur Wirtshaft und Technologie (BMWi)、すなわち連邦経済省の前身は 1917 年に設立された帝国経済局であり、経済の保護、促進、統制のための独立機関として設立された。同省の政策目標には「 経済の競争力を維持するための新技術の促進および技術革新」も含まれている。

（1） 組織

連邦経済省は、長官職の公務員が指揮する 8 つの監督局（DG）から成る。

- DG Ⅰ：経済政策
- DG Ⅱ：中小企業、工芸、サービス業、自由業、教育政策
- DG Ⅲ：エネルギー
- DG Ⅳ：貿易および産業、環境保護
- DG Ⅴ：対外経済政策および欧州統合政策
- DG Ⅵ：技術および技術革新政策；ドイツ新国家
- DG Ⅶ：遠距離通信および郵便
- DG Z：中央管理

各中央監督局は、副局長が率いる 4 つの監督局から構成されている。

BMWi はいくつかの下部機関を有しており、そのひとつに 郵政事業管理局がある。

主に郵政事業の監督機関が、情報テクノロジー分野での BMWi の責任を負う。郵政事業管理局は 1998 年 1 月 1 日に設立された。経済上の規制機能は、それまでは連邦郵政省によって行われていた。

元々は郵政省の下部機関であった連邦郵政局は、技術規制を担当していたが、1998 年、BMWi 下の新管理局に統合された。特に、料金、回線、ネットワーク・アクセス、ユニバーサル・サービスの保証における主要決定は、裁判システムにも似た意思決定で行われる。管理局は、遠距離通信市場の競合を維持し、適切かつ十分な遠距離通信および郵便サービスを全国的に提供することを任務とする。さらに、効率的で障害のないサービス不断の提供を確実に行わなければならない。

（2）デジタル署名法に基づく管理

ドイツデジタル署名法に基づき、郵政事業管理局（Regulierungsbehorde）は、デジタル署名の認証と認可を管理する。管理局は、この分野では BSI のサポートを受けている。管理局はドイツの「国内最上位認証機関」と称され、認証に関しては最高レベルの権限を有する。管理局はこの最上位認証機関（ルート CA）のプロセスを通じて、各認証機関にドイツ国内の実施権を与える。最上位認証機関をサポートするもう一つの団体は、TUV Informationstechnik GmbH である。管理局は、ドイツデジタル署名条例に基づくセキュリティ手段に関して以下の 2 件の文書を発行した。

- 認証機関のセキュリティ手段（：Security Measures for Certification Authorities）（参考文書B105）
- 技術コンポーネントのセキュリティ手段（：Security Measurs for Technical Components）（参考文書B106）

技術コンポーネントのセキュリティ手段の中で、推奨暗号アルゴリズムの要件を定義し

ている。

デジタル署名の認証の実施権を得ようとする民間の企業等の申請手続では、実際には公式の申請書はない。技術コンポーネントとセキュリティ・コンセプトの遵守を確認する文書のフォーマットは、申請者と管理局との間の合意によるものである。現時点での一般的な手続は以下のとおりである：

第1段階では、ドイツ電子署名法および条例の要件を満たしているかどうかを確認する。次の段階で、プロジェクトプランを作成する。いったんセキュリティ・コンセプトの基本が固まったら、申請者は管理局と協議するのが得策である。

（3） 最近の活動

最上位認証機関である郵政事業管理局から、以下の 3 つの団体が認証機関として認められている。

- ドイツ・テレコム社が 1998 年 12 月 22 日に実施権を授与された。
- ドイツ・ポスト社が 2000 年 2 月に実施権を授与された。
- Bundesnotarkammer（連邦公証会議所）が 2000 年 12 月 14 日に実施権を授与された。
- 他に 3～7 つの認証機関が 2001 年内に認可される予定である。

管理局に認証された製品には、Deutsch Telekom、Utimaco Safeware 社製の製品をはじめ、以下の製品が含まれる。

- Trust Center Key Generator（TC-SG）
- Trust Center Public Directory（OVTC）
- Function library TCrypt-TCM
- Telesec signature card PKS Card
- SafeGuard Sign&Crypt
- Smartcard reader HML 5010/5020/5021/5022
- Signtrust key generator
- Signtrust signing component SK-DPAG
- Signtrust signature card SEA Card
- Safeguard Sign&Crypt Software Development Kit
- Signtrust Zeitstempeldienst TSS-DPAG Version 1.0
- Signtrust Anwenderkomponecte eTrust Mail
- Time signature system TSS 400

1998 年以来、管理局はドイツ条例に基づくデジタル署名の適切な暗号アルゴリズムに関し、年次報告書を発行してきた。少なくとも数年間の使用に耐えられるような暗号アルゴリズムに関して報告している。（参考文書B108）

3. Bundesausfuhramt（BAFA）

Bundesausfuhramt（BAFA）、すなわち連邦輸出局も連邦経済省（BMWi）の下部機関である。連邦輸出局は以下の分野において、連邦政府の管理と監督業務を遂行している。

- 経済支援、輸入、エネルギー：連邦経済省は、経済政策を決定し、コミュニティ規模の規則作成を援助する責任を負う。この権限において、BAFA は経済政策を、国内の諸法、ガイドライン、条例および EU の要件に基づき企業および個人のための規則として具体化する。
- 対外貿易および決済法、対外貿易および決済条例、EC 二重条例：
  - 武器および二重用途製品の監督；武器関連の製品または技術の輸出が認可を必要とするかどうかの決定；輸出ライセンスに関する決定
  - 対外貿易および決済法の分野における、調査と刑事手続きのための専門知識の提供
  - 国際輸入証明書の申請に関する決定
  - EU 機関および国際輸出規制機関への参加
- 原子力エネルギー法：連邦環境・自然保全・原子力安全省の技術的および法的監視の下での、原子力エネルギー法に基づく輸出入ライセンスの申請に関する決定
- 武器規制法：武器の製造、輸送、販売の監督
- 化学兵器協定の履行法：化学兵器協定を実行する枠組み内の化学兵器産業における、化学兵器の特定データの収集および転送、国際査察の支援

ドイツの主要な輸出規制および許可機関として、BAFA はドイツの暗号製品の輸出に責任を負うが、BAFA は、暗号製品の性能もしくは技術基準に関して暗号認証も評価も行ってはいない。

Ⅲ. 参考文書

PartA：

1. *A European Initiative in Electronic Commerce ，April 1997*
2. *eEurope Action Plan，November 2000*
3. *Towards A European Framework for Digital Signatures and Encryption，October 1997（＊仮訳あり）*
4. *EC Proposal on Certain Legal Aspects of Electronic Commerce in the Internal Market*
5. *Directive of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*
6. *EESSI Steering Group Membership，September 2000*
7. *Organizational Chart for the ETSI*
8. *Organizational Chart for the CEN*
9. *Overview of the EESSI, First Consultative Meeting, February 1999*
10. *European Electronic Signature Standardization, EESSI Expert Team, July 1999*
11. *Final Report of the EESSI Expert Team, July 1999*
    （＊仮訳あり）
12. *ICT Standards Board EESSI Presentation, May 2000*
13. *EESSI Explanatory Document: Description of Deliverables，May 2000*
14. *ETSI ESI Working Group report at the Barcelona Conference, September 2000*
15. *Framework for EESSI Standards and Classes for Electronic Signatures，September 2000*
16. *ETSI Report Telecommunications Security: Electronic Signature Standardization Report，November 1998*
17. *Workplan for ETSI Electronic Signature Standardization，September 2000*
18. *ESTI Technical Specifications: Policy requirement for certification authorities*

issuing qualified certificates, December 2000

19. *ESTI Technical Specifications Qualified Certificate Profile, December 2000*
20. *ESTI Technical Specifications Time Stamping Profile, October 2000*
21. *ESTI Technical Specifications Electronic Signature Formats, December 2000*
22. *CEN/ISSS Report from the Brussels 1999 Meeting , December 1999*
23. *CEN/ISSS Workshop on Electronic Signatures Business Plan, Version 1.0, January 2000*
24. *E-SIGN Presentation*
25. *CEN/ISSS Report from the Stockholm Meeting, June 2000*
26. *CEN/ISSS Barcelona Conference Report, October 2000*
27. *CEN/ISSS Brussels Conference Report, November 2000*
28. *CEN/ISSS Brussels Conference Report, December 2000*
29. *CEN/ISSS: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures, January 2001*
30. *CEN/ISSS: Secure Signature-Creation Devices, version 'EAL 4', February 2001*
31. *CEN/ISSS: Secure Signature-Creation Devices, version 'EAL 4+', February 2001*
32. *CEN/ISSS: Security Requirements for Signature Creation Systems, October 2000*
33. *CEN/ISSS: Procedures for Electronic Signature Verification, January 2001*
34. *CEN/ISSS: EESSI Conformity Assessment Guidance, January 2001*
35. *Way forward - revised scope for Project Team on Area D, Nobember 2000*
36. *New disposition of comments on CWA draft Area F, Nobember 2000*
37. *Presentation on resolution of comments and CWA Draft on Area F, Nobember 2000*
38. *Explanatory memorandum concerning the two versions of the CWA Drafts on Area F, Nobember 2000*
39. *Disposition of comments on CWA Draft on Area G1, Nobember 2000*
40. *Disposition of comments on CWA Draft on Area G2, Nobember 2000*
41. *Inventory of European Economic Area Member State Strategies for implementation of European Directive 1999/93/EC, September 2000*

42. *Minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3 (4) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Nobember 2000*

43. *Revised proposed disposition of comments on CWA Draft on Area V, Nobember 2000*

44. *Proposed disposition of comments on CWA Draft on Area V, January 2001*

Part B：

1. UK Implementation of the EC Directive on Electronic Signatures,
2. Regulatory Intent Concerning Use of Encryption on Public Networks, February 1997
3. Licensing of Trusted Third Parties for the Provision of Encryption Services, March 1997
4. Secure Electronic Commerce Statement,
5. Building Confidence in Electronic Commerce – A Consultation Document, March 1999
6. Electronic Communications Bill, January 2000
7. House of Commons Library Research Paper on the Electronic Communications Bill, November 1999
8. Regulatory Impact Assessment for the Electronic Communications Bill, November 1999
9. Industry response to the Building Confidence in Electronic Commerce Consultation Document, April 1999
10. Industry response to the Promoting Electronic Commerce Consultation and draft Electronic Communications Act
11. Additional UK Industry Response to the Electronic Communications Act, October 1999
12. Electronic Communications Act Amendment to the Companies Act of 1985

13. DTI Consultative Letter on the Amendment to the Companies Act, March 1999

14. Summary of Response to the Amendment to the Companies Act

15. Summary of Responses to the Consultative Letter on the Amendment to the Companies Act , July 1999

16. Approval Profile for Registration Services, November 2000

17. Guidelines for the Verification of Identity of Individuals, November 2000

18. Guidelines for the Verification of Identity of Organizations, November 2000

19. Base Approval Profile , November 2000

20. CESG Approved Products Scheme products list

21. The Appointment of Commercial Evaluation Facilities , February 1997

22. IT Security - A Business Opportunity: An introduction for the IT industry: A general introduction to IT security in business and the UK ITSEC scheme., March 1996

23. Security Evaluation for IT Products: A vendors' guide to ITSEC: An introduction to the benefits and procedures of UK ITSEC certification, . March 1996

24. Certified Product List, April 2000

25. Description of the Scheme UKSP01, February 2000

26. Developers' Guide Part I (Roles of Developer in ITSEC) UKSP04/1, July 1996

27. Developers' Guide Part II (Reference for Developers) UKSP04/2, July 1996

28. Developers' Guide Part III (Advice To Developers) UKSP04/3, July 1996

29. UK IT Security Evaluation Scheme UKSP12, July 1996

30. Description of the CMS UKSP16 Part I, July 1996

31. Impact Analysis and Evaluation Methodology UKSP16 Part II, July 1996

32. Information Technology Security Evaluation Criteria ITSEC, June 1991

33. Common Criteria: An Introduction

34. Common Criteria Certification

35. Certification Report for Entrust, December 2000

36. French Implementation of the EC Directive on Electronic Signatures, May 2000

37. The 26th July Law, 1996

38. 1996 Draft of TTP Requirements

39. "Electronic Commerce", Lorentz task force, January 1998

40. March 1998 French regulations

41. Build a legislative framework to protect exchanges and privacy, January 1999

42. Prime Minister's announcement, January 1999

43. October 1999 Policy paper

44. Decree 99-200 of March 17, 1999

45. Decree 99-199 of March 17, 1999

46. Prime Minister's speech , August 1999

47. Evidentiary law and electronic signatures, February 2000

48. SCSSI Evaluation and Certification Procedures, June 1999

49. SCSSI Statement on Mutual Recognition, February 2000

50. Smart Card IC with Multi-Application Secure Platform Certificate, January 2001

51. Related Profile, November 2000

52. Transactional Smartcard Reader, February 2000

53. Related Profile, January 2000

54. Smart Card Integrated Circuit with Embedded Software, July 1999

55. Related Profile, June 1999

56. Intersector Electronic Purse and Purchase Device, April 1999

57. Related Profile, February 1999

58. Intersector Electronic Purse and Purchase Device (Version of Pilot Schemes), April 1999

59. Related Profile,]February 1999

60. Automatic Cash Dispensers/Teller Machines, April 1999

61. Related Profile, March 1999

62. Configurable Security Guard (CSG), April 1999

63. Firewalls V2.2, April 1999

64. Related Profile, September 1998

65. Firewalls V2.2, April 1999

66. Related Profile, September 1998

67. Carte a puce Billettique Avec et Sans Contact, April 1999

68. Smartcard Embedded Software, April 1999

69. Related Profile, November 1998

70. Smartcard Integrated Circuit Protection File, April 1999

71. Protection Profile Smartcard Integrated Circuit September 1998

72. SCSSI Centres d'Evaluation de la Sécurité des Technologies de l'Information , January 2000

73. Applications Oberthur Certification Report , January 2001

74. Micro-circuit ATMEL Certification Report , January 2001

75. Micro-circuit SLE66CX160M Certification Report , January 2001

76. SCSSI Certified Products , February 2001

77. German Implementation of the EC Directive on Electronic Signatures, May 2000

78. Interior Minister Kanther speech on April 28, 1997

79. Multimedia Law (of which the Digital Signature Law is Article 3), August 1997

80. Digital Signature Ordinance., November 1997

81. Summary of the Draft Technical Catalogues, November 1997

82. Bekanntmachung zur digitalen Signatur nach Signaturgesetz und Signaturverornung, September 1998

83. German Policy on International Recognition of Digital Signatures, August 1998

84. German Crypto Policy, June 1999

85. Act establishing a framework for electronic signatures (Signature Act), April 2000

86. Amendments to the Digital Signature Law, August 2000

87. Conditions for Electronic Signatures and for the Amendment of Further Legal Provisions, September 2000

88. An Ordinance on Electronic Signatures and on the Conversion of Fees to the Euro, November 2000

89. Official commentary on the Digital Signature Law Amendments, August 2000

90. German ICC's Draft Working Paper on Encryption,

91. German Consumer Association Statement

92. BSI Overview of its Assessment and Certification Programs, February 2001

93. BSI Mutual Recognition Policies,

94. BSI Application Notes and Interpretations, August 1998

95. BSI Certification: Information for Developers and Distributors, December 2000

96. BSI ITSEFs

97. Application for the Issuance of a Certificate by the BSI

98. BSI Documents on its Certification Programs,

99. German IT Security Certificates: Security of IT Products and IT Systems, March 2001

100. German IT Security Certificates: Security of IT Products and IT Systems (Expanded),December 2000

101. Certification Update List from February 2001

102. Certification Report for the Transport/S-2.0, October 2000

103. Certification Report for the Processor Resource/Systems Manager, February 2000

104. Certification Report for the Philips Smart Card Controller, January 2001

105. Security Measures for Certification Authorities , October 1998,

106. Security Measure for Technical Components, October 1998

107. Products certified by the Regulatory Authority , October 1998

108. Regulatory Authority Annual Paper on Suitable Cryptographic Algorithms December 2000