第２節　ドイツ及びＥＵにおける制度化に向けた動向

１　マルチメディア法

（１）マルチメディア法

認証機関（Zertifiziererungsstelle）に係る免許制（Lizenzerteilung）の導入等を内容とするデジタル署名（Gesetz zur Digitalen Signatur）を含む「情報・通信業務の条件を規制に関する法律（通称マルメディア法）」（Gesetz des Bundes zur Regelung der Rahmenbedingungen fur Informations und Kommunikationsdienste）が１９９７年７月に成立、８月から施行されている。

ア　マルチメディア法の概要

マルチメディア法の概要は次のとおりである。

ａ　目的

情報通信分野での企業活動を促進するため、最低限の法的枠組みを整備すること。

ｂ　基本方針

自由競争、利用者の正当な利益、公共秩序のバランスをとること。

ｃ　制定・施行年月日

１９９７年７月２２日制定。１９９７年８月１日施行（第７条のみ１９９８年１月１日）。

ｄ　担当省

ドイツ連邦教育科学研究技術省

ｅ　構成

全１１条。うち、第３条が「デジタル署名法に関する法律（SigG）」（以下「デジタル署名法」）。

イ　マルチメディア法制定時の議論について

マルチメディア法立法理由書によると、法制定時の論点及び解決策は次のとおりである。

論点１：いかにして電子認証の安全性を担保するか。

①　認証機関の免許制（任意的な資格認定制度）
②　署名者のみが秘密鍵を所有
③　技術コンポーネントの安全性検査
④　所轄官庁による認証機関の安全性に関する監督及び第三者機関による監査

論点２：残余リスクはなにか。

①　身分証明書の偽造等による電子署名の詐欺目的
②　認証機関の人的信頼性
③　秘密鍵保持者（署名者）の安全確保手続き

論点３：責任分担について、どう考えるか。

①　個々の故意・過失の度合いを鑑みて、一般私法に基づいて解決

論点４：技術進歩について、どう考えるのか。

①　法は一般的な枠組みのみを規定し、採用する技術方式は基本的に市場に委ねる。
②　複数の方式を使用する場合には、複数のＩＣカードまたは多機能カードの利用もしくは信頼できる第三者機関による相互認証が必要。

論点５：個人データ保護について、どう考えるのか。

①　秘密鍵はＩＣカードに記憶。ＩＣカードの安全性は耐タンパー性装置によっ

て担保。

② 電子署名用の個人データの収集には同意が必要。また、事前に同意を得た特定目的について必要最小限しか収集・利用してはならない。

また、連邦参議院からは、証明書発行は公共の仕事であるにもかかわらず、信頼性を十分に保証することなく私企業に委ねるものである及び適切な責任規定と賠償義務保険の義務を欠いている等の理由から、マルチメディア法から「第３条デジタル署名に関する法律」を削除すべきという意見が提出された。

（２）デジタル署名法及びデジタル署名法施行令の概要

デジタル署名法（SigG　１９９７年８月１日施行）及びデジタル署名法施行令（SigV　１９９７年１１月１日施行）の概要は次のとおりである。

ア　目的

① 電子認証制度の安全かつ効率的なインフラ整備

② 技術的安全性の保証

③ ユーザの啓蒙

イ　特徴

① 免許制

認証機関を運営すること自体は、事前許可を必要とされておらず、任意的な資格認定制度となっている。

(a) 所轄官庁による免許付与及び監督

所轄官庁は連邦電気通信・郵便規制庁（RegTP）とされている。所轄官庁は、アルゴリズム、パラメーターの適性などの技術コンポーネントの充たすべき要件に関するカタログ及び認証機関の安全装置に関するカタログ（Ma nahmenkatalog）を作成し、連邦官報に公示する義務を負う。それは、毎年見直され、連邦情報技術安全局（ＢＳＩ）のデータに基づき、経済・学術専門家の助言が反映される。

また、連邦電気通信・郵便規制庁（RegTP）は、国家最上位認証機関であり、マインツに設置され、デジタル署名法にもとづく電子認証サービスの免許付与と事業監督の役割を担う。

(b) 中立的な第三者による検査・監査（認証機関及び技術コンポーネントのそれぞれについて）

所轄官庁は、認証機関の審査・監査及び技術コンポーネントの検査を行う中立的な第三者機関をそれぞれ許可する。監査は２年に１度の割合で行われる。

検査については、「情報技術システムの安全性にかかる評価基準」（省庁合同報告１９９２年）に則って行われ、最新の技術水準を十分に反映しており、検査機関によりその安全性の程度が確認されれば、認可される。

② 充足要件

(a) デジタル署名の技術コンポーネントの充たすべき要件

技術的適性は少なくとも評価と公表の時点から６年間は継続しなければならない。その他の要件として、ユニークであること、秘密保持、複製・偽造・改竄・情報漏洩防止などのセキュリティ対策を備えていることなどが定められている。

独自の安全対策・新規導入は自由だが、ＢＳＩ（連邦情報安全技術局）は、ＩＴＳＥＣ（Information Technology Security Evaluation Criteria）の安全段階のうち、Ｅ４（主要なコンポーネント以外はＥ２）を求めている。（資料〇〇

参照）

(b) 認証機関及び証明書の充たすべき要件

認証機関に必要な事項について記した安全計画（技術コンポーネント一覧表、運用マニュアルなど）を作成し、所轄官庁または認可する第三者検査・監督機関による検査・監査を経て信頼するに足ると認められた場合に、連邦電気通信・郵便規制庁（RegTP）より免許が付与され、認証機関の署名鍵の証明書が発行される。

技術面以外に、法規の遵守・専門知識を有することなども審査の対象となる。

③ 個人データ保護規定

認証機関が電子署名用の個人データを収集するには、当該個人の同意が必要とされている。また、事前に同意を得た特定目的について、必要最小限しか収集・利用してはならない。署名者のみが秘密鍵を保有する。個人の署名鍵秘密鍵保持のため、あらかじめＩＣカードに格納された秘密鍵を認証機関に持ち込み、割当を受ける方式が望ましいとしている。

④ 国外の電子署名の有効性規定

⑤ 技術的柔軟性の確保

ウ 証明書発行プロセス

① 登録時の本人確認

認証機関は、連邦身分証明書、旅券またはその他適当な方法で申請者を認証する。申請には自署が必要とされ、仮名での登録が可能である。

② 署名鍵の割当

ユニークな一対の署名鍵が認証機関からユーザーに割り当てられる。原則として、署名鍵を交付する際には、ユーザーへの直接引渡し、引渡しの書面による確認が必要とされている。また、認証機関には、安全確保手続き、利用技術コンポーネント、有効期限及び新しい署名鍵への更新についての説明が義務付けられている。

③ 割当証明書の発行

認証機関はタイムスタンプをつけて割当証明書を発行し、ユーザに交付する。ユーザは割当証明が記入された秘密鍵を所持することになる。認証機関は、ユーザの要請に応じていつでも署名鍵を使用停止できるようにしなければならない。

④ 割当証明台帳の作成・管理

認証機関は割当証明台帳を作成・管理するとともに、割当証明書をいつでも誰でもオンラインで確認できる状態にしなければならない。

⑤ 有効期間

５年間

（３）デジタル署名法に基づき承認された検査・監査機関

１９９８年２月に出された連邦官報第３１号によると、デジタル署名法（SigG）及びデジタル署名法施行令（SigV）に基づき承認された検査・監査機関は次のとおりである。

ア デジタル署名法１４－４による技術コンポーネント検査のための、デジタル署名法施行令１７－４にもとづく公示

① 承認された機関

連邦情報技術安全局（Bundesant fur Sicherheit in der Informationstechnik）

② 仮承認された機関

・デービス・システムハウス・インフォーメーション・セキュリティサービス有限会社－認証機関（debis Systemhaus Information- Security Services GmbH－Zertifizierungsstelle）

・技術監査協会（ＴＵＶ）情報技術有限会社－情報技術安全検査機関（ＴＵＶ Informationstechnik GmbH Prufstelle fur IT－Sicherheit）

・技術監査協会（ＴＵＶ）製品サービス有限会社ＩＱＳＥ－情報技術安全検査機関（ＴＵＶＰＲＯＤＵＣＴ　ＳＥＲＶＩＣＥ　GmbH　IQSE－Prufstelle fr IT－Sicherheit）

仮承認は、これらの機関によって発行された、連邦情報技術安全局（ＢＳＩ）設置法４－４にもとづく安全証明書が、連邦情報技術安全局（ＢＳＩ）の安全証明書と同等の安全性を有するとの連邦情報技術安全局（ＢＳＩ）の確認書が連邦電気通信・郵便規制庁（RegTP）に提出されれば、正式承認となる。

イ　デジタル署名法

① 承認された機関

連邦情報技術安全局（Bundesant fur Sicherheit in der Informationstechnik）

② 仮承認された機関

・デービス・システムハウス・インフォーメーション・セキュリティサービス有限会社－認証機関（debis Systemhaus Information- Security Services GmbH－Zertifizierungsstelle）

・技術監査協会（ＴＵＶ）情報技術有限会社－情報技術安全検査機関（ＴＵＶ Informationstechnik GmbH Prufstelle fur IT－Sicherheit）

・技術監査協会（ＴＵＶ）製品サービス有限会社ＩＱＳＥ－情報技術安全検査機関（TUVPRODUCT SERVICE GmbH IQSE－Prufstelle fr IT－Sicherheit）

仮承認は、安全計画の領域における業務・技術上の実務経験によって一般的な専門知識が証明され（信用照会先を提出する）、デジタル署名法４－３－３に基づく連邦情報技術安全局（ＢＳＩ）と連邦電気通信・郵便規制庁（RegTP）による安全計画の審査によって、デジタル署名法及びデジタル署名法施行令にかかる特殊な専門知識が証明されれば、正式承認となる。

ウ　デジタル署名法にもとづく技術コンポーネントの安全性検査・監査を実施できる機関

連邦電気通信・郵政規制庁（RegTP）の把握している限りでは、デジタル署名法１４－４及びデジタル署名法施行令１７－１にもとづく技術コンポーネントの安全性検査・監査を実施できる状況にあるものは、次の９つの機関である。

・ＩＡＢＧ　ＩＴＥ（情報技術開発）部門（ＩＡＢＧ　ＩＴＥ－Abteilung）

・テレ・コンサルティング有限会社情報技術安全検査ラボ（Table-Consulting GmbH Pruflabor fur IT-Sicherheit）

・デービス・システムハウス・インフォーメーション・セキュリティサービス有限会社－認証機関（debis Systemhaus Information－Security Services GmbH－Zertifizierungsstelle）

・技術監査協会（ＴＵＶ）情報技術有限会社－情報技術安全検査機関

（TUV Informationstechnik GmbH Prufstelle fur IT－Sicherheit）
・技術監査協会（ＴＵＶ）製品サービス有限会社ＩＱＳＥ－情報技術安全検査機関
（ＴＵＶＰＲＯＤＵＣＴ　ＳＥＲＶＩＣＥ　GmbH　IQSE－Prufstelle fr IT－Sicherheit）
・コンピテンス・センター情報科学有限会社－情報技術安全検査機関
（Competence Center Infomatik GmbH Prufstelle fur IT-Sicherheit）
・VST　フォスロー・システム技術有限会社－情報技術安全検査機関（VST Vossioh System-Technik GmbH Prufstelle fur IT-Sicherheit）
・技術監査協会（ＴＵＶ）北ドイツ社団法人－ソフトウェア・エレクトニックラボ
（ＴＵＶ Nord e.V.Software & Elektronik Labor Gro e Bahnstra e）
・連邦情報技術安全局（Bundesant fur Sicherheit in der Informationstechnik）

（４）ドイツにおけるデジタル署名に関する状況

ア　最上位電子認証機関の設立状況

最上位電子認証機関は、マインツに設置され、デジタル署名法（SigG）にもとづき電子認証サービスの免許付与と事業監督の役割を担うこととなっている。連邦電気通信・郵便規制庁（RegTP）は、デジタル署名法にもとづく最上位認証機関の構築と納入について、欧州規模で公募入札を行った結果、ドイツテレコムが受注した。１９９８年９月２３日から、デジタル署名法に基づく所轄官庁である連邦電気通信・郵便規制庁（RegTP）に設立される最上位認証機関が稼動する。

イ　個別認証機関の設立状況

Deutsche Telecom AG は、１９９８年１０月末に、デジタル署名法（SigG）に基づく認証機関としての免許を取得し、ドイツ中に８００くらいの登録拠点を持つ予定とされている。その他の主要な認証機関への免許付与は、１９９９年末に行われると予想される。

ウ　法制の整備について

デジタル署名法（SigG）は、セキュリティ標準を保証するものであり、デジタル署名に自署に相当する法的効力を付与するための作業に取り組んでいる。社会保険の分野に使えるようにする最初の法改正が、１９９９年に行われている。今後、ドイツでは、伝統的な紙ベースの書類から電子文書へと移行するための法制度の整備がなされており、電子署名が自署と少なくとも同等、より協力な証拠となるように作業を進めている。

（５）電子署名に関する域内フレームワークに係る欧州評議会及び理事会指令の概要

電子署名に関する域内フレームワークに係る欧州評議会及び理事会指令（Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999）の概要は次のとおりである。

ア　目的

①　域内共通フレームワークの整備
②　財・サービスの自由移動の保証
③　技術進歩とグローバル化への対応
④　電子商取引市場におけるクロスボーダー取引の活性化と競争の促進
⑤　技術進歩とグローバル化への対応
⑥　電子商取引市場におけるクロスボーダー取引の活性化と競争の促進
⑦　信頼性とサービス提供の品質向上
⑧　自由競争の促進

⑨　電子署名の公的セクターにおける利用の促進

イ　特徴

①　市場アクセス（第３条）

・加盟国は、認証サービスの提供に関して、事前許可を必要とする規定を設けてはならない。これに反しない限り、加盟国は、認証サービス提供の信用補完を目的として、任意的な資格認定制度を導入し、運営することができる。かかる制度に関する要件はすべて、客観的で、透明で、均整が取れており、非差別的でなければならない。

・各加盟国は、自国内に設立され、公衆に対して高品質証明書を発行する認証機関の監督を行うために適切な制度を確立しなければならない。

・電子署名製品の一般に認められる技術標準の参照番号を付与及び公表。

・加盟国は必要な要件を付して、公的なセクターにおいて電子署名を利用することができる。当該要件は、客観的で、透明で、均整がとれており、非差別的でなければならない。かつ、導入部分に関連する特定の性質にのみ関連するものでなければならない。当該条件は、クロスボーダー・サービスの障害になってはならない。

②　電子署名の法的効力（第５条）

・加盟国は、高品質証明書が添付され、安全な署名作成機器によって作成された高水準電子署名が、「紙面上の手書き署名と同様に、署名としての法的要件を充足している」及び「法的訴訟における証拠として認められる」等の法的効力をもつことを保証しなければならないとしている。

・加盟国は、「電子署名が電子的形態であること」、「高品質証明書が添付されていないこと」、「指定認証機関が発行する高品質証明書が添付されていないこと」及び「高安全署名作成機器によって作成されたものではないこと」のいずれかの理由だけでは、訴訟手続きにおいて、電子署名の法的効力及び証拠力が否定されないことを保証しなければならない。

③　責任（第６条）

・最低限、加盟国は、高品質証明書を発行する認証機関が当該証明書を合理的に信頼したすべての者に対して、「当該高品質証明書に含まれるすべての情報が、同証書発行時点において正確であること、及び当証明書が高品質証明書に含むべき詳細事項をすべて含んでいること。」、「当該証明書発行時点において、当証明書の被認証者（署名者）が当該証書に記された署名照合機器に対応した署名作成データを所有していたこと。」、「認証機関が署名作成データ及び署名照合データを作成した場合に、両者が相補的に機能すること。」につき責任を負うことを確かにしなければならない（ただし、認証機関が自己に過失なきことを証明した場合には、この限りではない。）

・加盟国に対する、認証の失効手続きを適切に行わなかったために生じた損害につき、認証機関が責任を負うことを保証する義務、及び、認証機関に過失がなければ情報の改竄等の責任を負わないことを保証する義務を負う。

・加盟国に対する、高品質証明書の使用制限を明らかにし、それを超えた使用から生じる損害について認証機関の責任を免除する義務を負う（ただし、その制限は第三者に認められるものでなければならない）。

・加盟国に対する、高品質証明書の取引限度額を明らかにし、それを超えた取引

から生じる損害について認証機関の責任を免除する義務を負う（ただし、その制限は第三者に認められるものでなければならない）。

④　国際的側面（第７条）

加盟国は、第三国において設立された認証機関が発行する高品質証明書が、「当該認証機関が、本指令に書かれた要求を充たし、加盟国の任意的な資格認定制度において認定されている」、「域内で設立され、本指令に書かれた要求を充たす認証機関が、自らの証明書を保証する」、「当該電子証明書又は認証機関が、欧州共同体と第三国あるいは国際組織との間で、二国間協定又は多国間協定に則って認められている」のいずれかの要件を備えている場合、域内において設立された認証機関が発行する証明書と法的に同価値とみなされることを保証しなければならない。

⑤　データ保護（第８条）

・加盟国は、監督機関、検査・監査機関及び認証機関が１９９５年１０月２４日の欧州議会とヨーロッパ理事会による指令95/46/EC(EU個人データ保護指令)を遵守することを保証しなければならない。

・加盟国は、公衆に対して証明書を発行する認証機関が、データ主体から直接に同意を得た場合又はデータ主体の明示的な同意を得た上でのみ、かつ、証明書の発行・管理に必要最小限のみ、個人データを収集することを保証しなければならない。データ主体の明示的な同意なくして、他の目的で個人データを収集・処理しなければならない。

・国内法に基づく仮名の使用に与えられる法的効力に反しない限りにおいて、電子証明書で仮名が使用できるようにする。