タイムビジネスに関する
ドイツ動向調査
報告書

平成１６年７月

タイムビジネス推進協議会

はじめに

近年の情報通信の急速な普及に伴い、自由な情報活用を可能とする高度情報通信ネットワーク社会の構築が急務となってまいりました。電子商取引や電子政府はその中心的な役割を担い、国民の利便性の向上に大きな期待がよせられているところでありますが、一方では電子社会に特有なさまざまな脅威も存在しております。電子社会に特有な脅威のうち、特に電子データの特性を利用した「不正行為」や「情報システムの障害」に対しては、ネット上での「信頼できる時刻」の利用が不可欠となります。

タイムビジネス推進協議会では、「電子データの非改ざん」や「ネット上で取引が行なわれた正確な時刻」の第三者的証明を可能にするため、ネット上での標準時配信サービスや時刻認証サービス（いわゆるタイムスタンプサービス）を「タイムビジネス」と称し、安全な電子社会基盤構築に向け、民間事業者、大学、研究機関等が結束し、タイムビジネスの調査研究や各種ガイドラインの整備、実証実験等を通じ、タイムビジネスの普及に向けて取り組んでまいりました。最近では、政府・自治体の電子調達システムや一部の民間企業において、タイムビジネスの利用が広まりつつありますが、制度面での枠組み整備等の課題も残されております。

このような背景をうけ、タイムビジネス推進協議会では、タイムビジネスの先進事例として、ドイツにおけるタイムビジネスの実態調査を行なうこととなりました。ドイツでは、1997 年に制定された「電子署名法」をうけて、特にタイムスタンプを中心としたビジネスが登場しております。また、ドイツを含む EU 域内では、各種サービスの自由な流通が認められており、EU 各国への影響を与える EU 電子署名指令についても調査を行ってまいりました。

本調査が、更なるタイムビジネスの普及に寄与し、安全な電子社会基盤構築の一助となれば幸いです。最後に、本調査にあたって多大なご支援、ご協力をいただいた訪問先の方々、ドイツ日本大使館、神戸大学米丸先生を始めとする本報告書の執筆者の方々に深く感謝し、お礼を申し上げる次第であります。

平成 16 年 7 月

タイムビジネス推進協議会
会長　　大橋　正和

目 次

１．本調査の目的

安全な電子社会の構築に向け、「電子データの原本性」や「ネット上で取引の行なわれた時刻」を証明するために、タイムビジネスへの注目が高まりつつあります。こうした背景をうけて、タイムビジネス推進協議会では、国内利用動向の調査や各種ガイドラインの整備等を行なってまいりましたが、更なるタイムビジネスの制度的な枠組みを確立するために、タイムビジネスに関して法整備を行なっているドイツの実態を調査することとなりました。今回の調査では、ドイツ電子署名法に詳しい神戸大学の米丸教授に解説をいただくことで、より理解度の高い内容を目指しております。

２．調査スケジュール

3 月 17 日（水）　出国：結団式　成田空港発～フランクフルト着

3 月 18 日（木）　郵電規制庁訪問

3 月 19 日（金）　AuthentiDate 社訪問

3 月 20 日（土）　Leuven　Universiteit　訪問

3 月 21 日（日）　移動

3 月 22 日（月）　連邦経済労働省、連邦公証人会訪問

3 月 23 日（火）　まとめ　帰国の途へ　ベルリン空港⇒フランクフルト空港発

3 月 24 日（水）　帰国：成田空港着

３．参加メンバー

(順不同・敬称略)

団　長	大橋　正和	中央大学総合政策学部長、総合政策学部教授・工学博士
副団長	米丸　恒治	神戸大学　法学研究科教授
	中間　　弘	総務省　情報通信政策局技術政策課研究推進室課長補佐
	内藤　隆光	アマノ株式会社　e-timing ビジネス開発部　理事
	米沢　実	アマノ株式会社　総合企画室営業企画　理事
	三谷　慶一郎	株式会社 NTT データ経営研究所 情報通信コンサルティング部　部長
	鳥山　裕史	独立行政法人通信総合研究所　電磁波計測部門 タイムスタンププラットフォームグループ　グループリーダー
	遠藤　宏	株式会社 NTT データ　ビジネス開発事業本部 セキュリティビジネスユニット　ビジネスユニット長
	櫻井　徹	株式会社 NTT データ　技術開発本部　シニアエキスパート
	谷川　嘉伸	株式会社日立製作所　システム開発研究所　第７部　研究員
	中嶋　勝治	セイコープレシジョン株式会社 ソリューション事業本部　ソフト開発部　副主査
	島　　成佳	日本電気株式会社　システム基盤ソフトウェア開発本部　主任
	林　　誠一	NTT データセキュリティ株式会社　企画部　部長
	小関　健	上智大学　理工学部電気電子工学科　教授
	田邉　俊史	株式会社 NTT データ経営研究所 情報通信コンサルティング部　コンサルタント
事務局	大西　祥浩	財団法人テレコム先端技術研究支援センター 研究企画部　研究企画部長
事務局	刑部　正敏	財団法人テレコム先端技術研究支援センター 研究企画部　調査役

４．総括報告

４．１　電子署名法制とタイムスタンプに関する規定の整備

ここでは、まず電子署名およびタイムスタンプ関連の法制度の整備がどのように進められてきているかについて、その内容を含めて見ておくことにしたい。[1]

４．１．１　マルチメディア法におけるデジタル署名法の整備

(1)　マルチメディア法

まず、世界に先駆けて総合的なサイバースペース基盤法制を整備したドイツのいわゆるマルチメディア法、およびそれに含まれているデジタル署名法の内容とその後の展開を紹介することにしよう。ドイツは、このマルチメディア法によって、ネットワーク上の様々なサービスを包括する情報・通信サービス(「テレサービス」という)について、サイバースペースの基盤整備をし、統一的な法規制を行った代表的な国となった。同法によって、新たな情報サービスおよび通信サービスの利用に関する法的な基礎が与えられ、新たなサービスを創造するための法的な大綱条件が整備されたといってよい。同法は、サイバースペースにおける法規制の基盤となる、いわばサイバー法の基礎としての性格を持つものである。

いわゆるマルチメディア法とは、ドイツにおいて 97 年 8 月に施行された「情報サービスおよび通信サービスのための大綱条件の規律のための法律」[2] のことである。同法は、3 つの新法の制定と、6 つの法律の改正を内容とするオムニバス法であり、全 11 箇条からなっていた。

(2)　デジタル署名法

いわゆるマルチメディア法の３条によって、デジタル署名法(Gesetz zur digitalen Signatur；Signaturgesetz；SigG)が制定された。

オープンなネットワークであるインターネットを介した通信では、データの改ざんや、

---

[1] 以下の報告をまとめるにあたっては、担当者の米丸恒治が過去に公表してきた次に掲げる論文、翻訳などを利用していることを予めお断りしておく。米丸恒治「ドイツ流サイバースペース規制－情報･通信サービス大綱法の検討－」立命館法学 255 号 141-194 頁(1998 年)、同「ドイツ・デジタル署名法と電子認証－サイバースペースの不確定性克服の制度基盤の検討－」立命館法学 256 号 31-73 頁(1998 年)、同「2-2-A6　消費者保護」、「2-2-C1　認証」、「2-2-C3　電子署名－イタリア　ジョバンニ・ツイカルディ」(訳)、「2-2-C4　電子署名－アメリカ　トーマス・J・スミーディングホフ／ルース・ヒル・ブロウ」(訳)(サイバー法研究会編『サイバースペース法』日本評論社)119-124、183-188、194-198、199-204 頁(2000 年)、同「情報の国際間流通と法制度-ドイツ・マルチメディア法」(多賀谷一照・松本恒雄編『情報ネットワークの法律実務』第一法規 6251-6263 頁(2002 年)、同「ドイツにおける電子政府の現状と電子的行政手続法」行政管理研究 101 号 19-37 頁(2003 年)。拙稿としているのは、これらをさす。

[2] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz；IuKDG) v. 22.7. 1997 (BGBl. I S. 1870). 同法については、前掲拙稿・立命 255 号 141 頁以下参照。3 つの新法については、同 179 頁以下で拙訳を掲げた。

特定の人物へのなりすましなどの犯罪行為または不正行為が行われやすいため、それらを追跡または検査する方法の開発・実用化が追求されてきた。その中で、いわゆるデジタル署名は、非対称暗号技術を利用して、ネットワークを通じて送受信されるデータまたはファイルが、真正なものであるかどうか、すなわちそのデータとしての完全性(改ざんされていないこと、脱落のないこと)と、通信の相手方の本人確認をするためのネットワーク上の技術である。アメリカ合衆国の州レベルの立法、たとえばユタ州デジタル署名法などに続き、国家レベルでは、ドイツのデジタル署名法が代表的な立法例であった。電子商取引や電子政府を支える PKI(公開鍵認証基盤)の構築に関わり、このデジタル署名法は、現在に至るまで重要な基礎をなすものであるので、以下、その内容をみておこう。

① 概要

ドイツのデジタル署名法は、デジタル署名のためのキーの生成、および公開署名キーが特定の人物のものであることを証明書により証明し、証明書の有効性を検証させるサービスを行う認証機関を、民間の組織により行わせることとしており、その上で、認証機関の事務、認証機関としての活動の開始要件(免許制度)、顧客との関係での義務、信頼性のあるデジタル署名を実現するための技術的およびセキュリティ上の要件などについて定めをおいていた。署名法は、後述のようにデジタル署名自体の実体的な効力については規定を置かず、むしろ信頼性ある署名手続、署名の検査手続を作り上げるための制度基盤を整備することを目指した行政法的規制を中心としていた。

同法によればデジタル署名とは、「私的署名キー(privater Signaturschlüssel)によって生成されたデジタルデータに対する印(Siegel)であり、認証機関(Zertifizierungsstelle)または第３条による行政庁の署名キー証明証(Signaturschlüssel-Zertifikat)が備えられたそれに対応する公的キーを用いることにより、署名キーの所有者およびデータが改ざんされていないことを認識させるもの」と定義されていた(２条１項)。

署名法は、デジタル署名されたデジタルデータ、電子文書の法的な効果(たとえば民法典の要求する契約書式として認められるかどうか)およびその訴訟法上の証拠能力については、規定をおいておらず、署名法の要件を満たすデジタル署名(免許を得た認証機関を利用するもの)は、技術上およびセキュリティ上の要件を満たすことが保証されることによって、事実上安全なものとして推定される(１条１項)効果をともなう[3]とされていた。

また、署名法上、タイムスタンプ(Zeitstempel)とは、「認証機関に特定のデジタル・データが特定の時点に提出されたということについての認証機関によるデジタル証明で、デジタル署名を付されたもの」と定義されていた(２条４項)。

② 認証機関の事務と免許

[3] Alexander Roßnagel, Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, S. 3312 ff.

デジタル署名法の規制の重点は、デジタル署名そのものよりも、むしろ認証機関におかれていた。同法のいう認証機関とは、「公的署名キーがある自然人のものであることを証明し、かつそのための本法第４条による免許を有する自然人または法人」(２条２項)と定義され、その活動の中心は、公的署名キーについての証明証の発行・管理、効力停止(８条)、ならびにデジタルデータにタイムスタンプを付与し、当該データの時間的な定位を行うタイムスタンプサービス(９条)である。「認証機関」として活動するためには、４条により、電気通信規制行政庁の免許が必要とされた。しかし無免許で活動した場合でも、罰則は設けられていなかった[4]。

97 年の署名法上は、タイムスタンプは、認証機関の義務的なサービスとされ、認証機関は、ユーザーの求めに応じてタイムスタンプを付すことが義務づけられていた。署名法９条は、「認証機関は、デジタルデータに求めに応じてタイムスタンプを付さなければならない。第５条第５項第１段および第２段は、これを準用する。」との規定である。この規定では、まさにユーザーの求めに応じて、認証機関がタイムスタンプを付すことが義務として定められていた。電子署名の利用にとって必要不可欠なものとしてタイムスタンプが位置づけられていたことが注目される。

なお、ここで参照されている第５条第５項第１段および第２段とは、「認証機関は、認証活動の遂行のために信頼のおける者をおかなければならない。署名キーの準備および署名の生成のために、認証機関は、第１４条[5] による技術的な装置をおかなけれ

---

[4] 後述のように、現行法では、免許制は廃止され、届出制と任意の認定制度を組み合わせている。現行法では、無届けでの認証機関の活動には過料を課すこととしている(21 条)。

[5] 〔技術的装置〕

第一四条　　署名キーの生成および保存ならびにデジタル署名の生成および検査のためには、デジタル署名の偽造および署名されたデータの改ざんを確実に認識可能にしかつ私的署名キーの不正な利用から保護する、セキュリティ措置を施された技術的装置を必要とする。

(2)　　署名されるべきデータの表示のためには、デジタル署名の生成をあらかじめ一義的に示しかつどのデータにデジタル署名が関連しているかを確認させるセキュリティ措置を施された技術的装置を必要とする。署名されたデータの審査のためには、署名されたデータが変更されていないかどうか、どのデータにデジタル署名が関連しているか、およびどの署名キー保有者にデジタル署名が属するかを確認させるセキュリティ措置を施された技術的装置を必要とする。

(3)　　署名キー証明証を第五条第一項第二段により審査しうることのできるまたは呼び出すことのできる技術的装置にあっては、証明証目録を不正な変更および不正な呼び出しから保護するための措置を必要とする。

(4)　　第一項ないし第三項による技術的装置にあっては、技術の水準に照らし十分に審査されていること、および所管行政庁により承認された機関により必要条件をみたしていることを確認されていることを必要とする。

(5)　　ヨーロッパ連合の他の構成国においてまたはヨーロッパ経済地域についての協定のその他の締約国において通用している規制もしくは要件にしたがい適法に製造されもしくは流通しており、かつ同等のセキュリティを保障された技術的装置にあっては、第一項ないし第三項によるセキュリティ技術上の仕様にかかわる要件は満たされているとみなす。説明資料を付された個別事例においては、所管行政庁の求めに応じて、第一段の要件が満たされていることが証明されなければならない。第一項ないし第三項にいうセキュリティ技術上の仕様に関する要件の証明のために所管行政庁により承認された機関の確認証の提示が定められている場合において、ヨーロッパ連合の他の構成国またはヨーロッパ経済地域についての協定のその他の締約国において許可された機関による確認証についても、その機関の審査報告書の基礎とされている技術的要件、審査および検査手続が所管行政庁により承認された機関のそれと同等のときは、それを考慮する。

ばならない。」という規定である。職員および技術的な装置の点で、タイムスタンプについても、電子署名についてと同様の要件が課されている。[6]

認証機関は、規制行政庁により免許され認証活動を行うが、その際に用いるデジタル署名は、規制行政庁により認証され、署名キー証明がなされる(４条５項)。ドイツ署名法上は、認証機関が用いる署名キーについての認証(根幹認証)を行う規制行政庁と認証機関との２段階的な認証構造がとられている[7]。

認証機関の個別の免許要件等の細目は、デジタル署名法 16 条にもとづくデジタル署名令(Signaturverordnung)[8] の中で定められている。

③　認証機関の義務

署名法は、信頼性あるデジタル署名を実現するために、認証機関に対していくつかの義務を課していた(これらは、現行法でもほぼ同様である)。

まず、署名法５条は、証明証の付与に関して、確実な、申請者の本人確認義務、公的署名キー証明証をネットワーク上でアクセス可能にしておく義務(以上１項)、証明証のデータの偽造または改ざんからの防止義務、秘密保持義務、および私的署名キーの認証機関での保存の禁止(以上４項)を定め、信頼性ある認証業務遂行のための職員配置義務を課している他、技術的な設備も１４条の基準に従い装備することを義務づけている(５項)。以上の義務により、民間によっても確実な本人確認に基づく安全確実な電子署名の基礎が確保される。

第２に、６条は、認証機関に、署名の信頼性確保のためのユーザーへの教示義務を課している。

その中には、タイムスタンプの利用についての教示事項も含まれ、同条を具体化する署名令４条の中には、「署名されたデータの利用に関し日時が重要な意味を持ちうるかぎりでは、タイムスタンプを付すものとすること」(５項)、および「データが比較的長期にわたって署名された形式で保たれる必要があるときは、１８条により、新たにデジタル署名を付すものとすること」(６項)という二つの教示事項が義務づけられていることが注目される。

特に、電子署名済みのデータが、時間の経過と技術の進歩によって、署名時に利用されたアルゴリズムが危殆化し、偽造が可能になることによって、署名時の真正性を

---

[6] さらに具体的な要件としては、タイムスタンプの生成に関わる職員の信頼性の要件(旧署名令 10 条)、タイムスタンプの生成に関わる技術的な装置の無権限者からの保護(旧署名令 11 条)、タイムスタンプ生成に関わる技術的な装置の要件(旧署名令 16 条５項：「署名法９条によりタイムスタンプが生成される技術的な装置(コンポーネント)は、タイムスタンプ生成時に通用している法律上の時が、変造されることなくこの中に取り込まれるような仕様のものでなければならない。この技術的なコンポーネントのセキュリティ技術上の変更は、運転者に認識可能になるものでなければならない。」との規定を置いていた。

[7] 現在でも、認定認証機関については、旧デジタル署名法のしくみが基本的に引き継がれ、２段階的な認証構造も維持されている。

[8] Verordnung zur digitalen Signatur (Signaturverordnung –SIGV) v. 22. Okt. 1997 (BGBl. I S. 2498).

保ち続けられない(偽造されたものではない、改変がない、ということを証明できない)ために、アルゴリズムが危殆化する前に、新たな適切なアルゴリズムとパラメータを用いて再署名(新署名)しなければならないとされており、97 年法制定当時から、この点についての配慮がなされていた。

６条の教示義務の中には、「認証機関は、申請者に対して、デジタル署名を付されたデータについて、すでに存する署名のセキュリティ度が時間の経過により低下する前に、必要があれば新たに署名をしなおさなければならないことを指示しなければならない。」という規定が含まれ、認証機関の義務として、再署名(新署名)の教示を行うことを求めている。また、これに対応する規定として、電子署名令では、１８条で、再署名についての規定をおいている(後述)。

第３に、認証機関は、その発行した証明証および技術的な装置について、常にその審査が可能なように記録を保持する義務も課されている(１０条)。署名令 13 条 2 項の記録保存義務により、35 年までは、署名法１０条に基づく文書の保存が義務づけられるため、その間は署名の検証が可能になっている。

第４に、認証機関の活動が公共性を持つ社会的な活動であることから、法１１条は、認証機関が活動を中止するときの行政庁への報告義務、他の機関に業務を引き継いでユーザーへのサービスが停止しないよう手配する義務、または証明証の効力を停止する義務を課している。また、認証機関の破産などの場合も、郵電規制庁が証明書等を引き継ぐことにより、既発行の証明証の検証が保証される(１３条４項)。この義務により、認証機関の活動の継続性とその公的統制が確保される。

第５に、認証機関のデータ保護に関する義務として、個人関連データの必要最小限原則を定め、その目的外使用を制限している(１２条１項)。なお、ドイツの署名法上は、仮名による署名も認められており、仮名での署名キー証明の取得も認められているが、その際、認証機関は、国家機関による犯罪捜査等の目的での個人データの引渡要求に応じなければならない義務も課されている(同２項)。

④　署名法とタイムスタンプの役割

電子署名は、デジタルデータの完全性と署名者の本人性を確認することを可能にするが、それだけでは、いつの段階で署名がなされたのかは確認することができない。そのため、証明書の効力が取り消れたり、その効力が切れてから、電子署名を行って、ファイルの時刻を改変すれば、電子署名の偽造が可能になる。こうしたリスクを極小化するためには、電子署名に際し、タイムスタンプを付することが求められる。署名法は、こうした考慮に基づき、電子署名とタイムスタンプの利用は不可分のものとしてサービス提供を求めていた。

電子署名の利用に関わり、タイムスタンプが必要とされる理由は、大きく次の 3 点にまとめられる。

1） 第一の理由として、そもそも、時刻が重要となる署名を行い、書類の送受信上で送受信時が重要となるときに、それを証明するためにタイムスタンプが必要であること。タイムスタンプを用いなければ、コンピュータの時刻を任意に調整することによって、日時を任意に変更できるために、日時の証明をすることができないため、第三者による客観的な日時の情報の付与を受け、それを偽造できないように確定するところに、このタイムスタンプの存在理由がある。

2） 第二の理由として、電子署名の性格上、電子署名の基礎となる証明書の有効期間が切れ、または証明書の有効性が失効することが予定されているが、証明書の有効期間が切れたり失効してから、その証明書に基づく署名を行い、署名日時を偽造すると、事後的に証明書の有効期間内に署名が行われたかのような偽造が行われうる。特に、署名者の署名カードが盗まれるなどして、証明書の失効手続を行ったときに、その署名カードの利用権限がない者が、署名が失効前に行われたかのようにして署名をなす可能性がある。こうした可能性は、証明書の有効期間内に行われた署名であることをタイムスタンプ付きで署名することで限定することによってしか、防ぐことはできないと考えられている。こうした偽装を防ぐためには、正規の署名時にタイムスタンプを利用することでしか、対応することはできない。

3） 第三の理由として、電子署名されたデータの長期保存に関わり、タイムスタンプが必要となる。97 年法では、すでに制定当初から、長期保存の際に、署名時の署名が時間の経過と技術進歩により偽造される可能性が出てくることを想定し、そのための対策として、まだ署名等時の署名が安全なうちに(偽造可能にならないうちに)タイムスタンプを含めて、新たに安全な署名を重ねることにより(再署名、新署名)、署名時のデータの真正性・完全性を保証する対策を想定しており、その点についてユーザーに対し認証機関が教示する義務も署名法６条〔教示義務〕で定め、さらに、署名令１８条の中に、このための手続を定めていた。

署名令１８条「〔新デジタル署名〕 データが、その作成および検査のために利用されたアルゴリズムおよび付属のパラメータが１７条２項により適切であると判断される期間よりも長期間にわたって署名された形式で保たれる必要があるときは、そのデータには、アルゴリズムおよび付属のパラメータの適性が失われる前に、新たなデジタル署名を付さなければならない。新デジタル署名は、新たなアルゴリズムまたは付属のパラメータでなさなければならず、以前のデジタル署名を含みかつタイムスタンプを有していなければならない。」このように当時から、長期保存のためには、新署名による対応（カプセリング）が必要であり、そのためにタイムスタンプが利用されなければならないことが明確に規定されていたのである。

なお、この 97 年法の段階では、電子署名に不可欠なサービスとして、タイムスタン

プサービスは、認証機関の義務的なサービスとされていたが、次のＥＵ指令の国内措置としてなされた改正によって、ＥＵ指令に合わせるかたちで、タイムスタンプが義務的なサービスから任意的なサービスとされることになった点が指摘されている。

４．１．２　ＥＵ電子署名指令

(1)　ＥＵ指令の影響

以上のような内容のマルチメディア法は、サイバー法の基盤整備法制として国際的に注目された。特に、国境の壁のない人、モノ、資本の自由な流通が保障された内部市場を形成しようとしてきたヨーロッパ連合(EU)では、ドイツのマルチメディア法など各国の法整備に刺激され、サイバースペースでも欧州全域での共通の考え方にたつ基盤整備の必要性が認識されるに至った。そしてドイツなどの国内法整備後に進められた EU での立法準備作業の結果、いわばヨーロッパのマルチメディア法制ともいうべき 2 つの指令が制定された。それは、欧州版電子署名法たる、EU 電子署名指令「電子署名のための共同体の枠組に関する 1999 年 12 月 13 日の欧州議会および欧州連合理事会の指令 1999/93/EC」[9]と、欧州版テレサービス法とでもいうべきいわゆる EU 電子商取引指令「内部市場における情報社会サービス、特に電子商取引の一定の法的観点に関する欧州議会および欧州連合理事会の 2000 年 6 月 8 日の指令 2000/31/EC(電子商取引指令)」[10]である。このうち、電子署名指令は、2001 年 7 月 19 日までに、構成国の国内法上必要な国内措置をとることを求めている。ＥＵ加盟国は、この時点までに、指令に適合的な内容の国内法制整備を義務づけられた。

電子署名指令は、ドイツのデジタル署名法のような一定の技術的組織的要件を満たす認証機関を免許制で個別的に認める原則をとらず、電子署名製品およびサービスの自由流通を原則とし、安全な署名のために指令の定める一定の条件を満たすものであれば、事前の許認可制に服させることなくそれを法的に認めることを求めている(３条)。そのために、前述したような免許制をとるデジタル署名法は、改正を余儀なくされることになった。

---

[9] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.1.2000, p. 12. 同指令の拙訳として、拙訳「ＥＵ電子署名指令」立命館法学 268 号 276 頁以下(1999 年)参照。後掲の資料参照。

[10] Directive 2000/31/EC of The European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, p. 1. 同指令の拙訳として、拙訳「ＥＵ電子商取引指令」立命館法学 278 号 224 頁以下(2001 年)参照。

(2) 電子署名指令の特徴

指令の特徴は、次の点である。

① 電子署名の法的効力の承認

指令は、電子署名が、電子的な形式によるものであるだけの理由で、手書きの署名とその効力において差別されてはならないことを定める(５条２項)。そして電子署名製品、証明証および認証サービスプロバイダ(認証サービス事業者)が、指令の定める特別な要件を満たせば(指令は、それぞれ「先進電子署名」、「安全署名作成装置」、「適格証明証」として区別している)、それらにより作成される電子署名を、法的には手書き署名と同等の効力を持つものとして扱うことを求めている。また手書き署名が、争訟手続において証拠としての証明力を認められるのと同様に、電子署名も証拠能力が認められるべきであることを定めている。

こうして指令は、手書きの契約書等に記された署名と電子署名を基本的な法的効力の点で同等のものとして扱うことにより、電子的な通信の中での電子署名の法的意義を認めるのである。

② 電子署名製品および認証サービスの自由な流通

指令は、電子署名に関する製品が、事前の許認可なく自由に流通させることができ、認証サービスも許認可なしに営むことができることを定める(３条)。特に、EU においては、たとえばある構成国に属する認証サービスプロバイダは、他の構成国で改めて許認可や事前の統制を受けることなく、そのサービスを提供することができることを保障することにより、EU の内部市場における製品とサービスの自由流通を保障することとしている。この点は、従来から、人、もの、資本の自由流通により内部市場を形成してきた EU の共通市場政策の延長といってよい。

③ 認証サービスプロバイダの責任

第三に、指令は、認証サービスプロバイダの責任についても、最小限の規定をおいている(６条)。それが発行する証明証に記載された事項についての法的責任を明示している。責任の明確化を通じて、認証サービスの信頼性を高めると同時に、自由な流通を保障された証明証および認証サービスについての最低限の基盤的な保障を行い、また一方でプロバイダが参入をい縮しないような効果もめざされているものと思われる。

④ 技術中立的な枠組

第四に、指令は、電子署名の信頼性を高めるための技術については、技術中立的なアプローチを取っている。署名作成データと署名検査データの二組のデータを用いて、署名の確認を行い、また認証サービスプロバイダにより発行される証明証を用いて署名者の同一性を確認するスキームを取ってはいるが、技術的には非対称暗号技術によるデジタル署名やバイオメトリクスを利用した署名技術など、技術的な発展に応じた柔軟な法的枠組を用意している。

⑤　適用の重点

指令は、その適用対象の重点を、電子データの送信者の特定を目的として公に発行される証明証、認証サービスにおいている。したがって、契約当事者間または既知の通信当事者間で、技術的な通信方式について合意が得られているような場合にも基本的にはその効力を認める(５条２項、考慮事項(16))が、多くの規制をおいているわけではない。たとえば、いったん当事者間で相互の信頼の下に通信が成立した後は、共通キー方式の暗号技術を用いた通信が行われることも当然予想されるし、それを指令は排除するものではない。その場合も、通信に付される署名データは、電子署名としてその法的な効力は認められることになろう。企業内、同一組織内のイントラネットなどでの通信方式についても同様である。

⑥　国際的な観点

指令は、EU 域内の共通の制度枠組を示すと同時に、域外との通信についても言及している。それによれば、第三国との関係では、証明証および認証サービスの二国間または多国間での相互認証により、相手国の認証サービスプロバイダが発行した証明証を相互に受け入れ、法的にその効力を認めることとしているのである(七条)。

(3)　署名の種類

電子署名指令上は、前述のように技術中立的な規定となっているが、その規定などから、次のような電子署名の種類があることになっている。

①　第１段階：「電子署名(electronic signature)」　指令２条１号の定義

「別の電子データに付加されまたは論理的にそれと結びつけられておりかつ真正確認の方法として用いられる電子的形式のデータ」。したがって、手書の署名をスキャンして画像としてはりつけたようなものもこれにあたる。

②　第２段階：「先進電子署名(advanced electronic signature)」同２条２号の定義

以下の要件を満たす電子署名　「(a)それがもっぱら署名者のみに帰属させられており、 (b)署名者の同一性確認が可能であり、(c)署名者がその唯一の統制の下に保持することのできる手段により作成されており、(d)事後的なデータの変更を認識させ得るように、その関連するデータにリンクされている」

ここでいう先進電子署名は、セキュリティを確保するためのインフラは予定しておらず、また PKI の要件も定められていない。たとえば、純粋にソフトウェアの　みに基づく署名、PGP を利用した署名も、この分類に属するとされる。

③　第３段階：いわゆる適格電子署名(qualified electronic signature)

「先進電子署名」の要件に「加えて」指令５条１項および付属書１ないし３[11]に示

[11] 付属書の１ないし３は、電子署名が手書の署名と同等のものとして扱われるために必要なセキュリティのインフラを定めるものとされており、付属書１は「適格証明証の要求事項」を定め証明書が「適格」なものとして扱われるための要求事項を列挙し、付属書２「適格証明証を発行する認証サービスプロバイ

された加重要件をみたす署名。手書の署名と同等と扱われる安全性の高い署名。

④　追加要求事項：

指令では、認証サービスの水準の向上を目標として任意の認定制度が認められ、さらには、公共部門に関しては明確に指令３条７項により追加要求事項を求めることも明確に認められている。結果的に、こうした追加要求事項をみたす署名が、一般には最高水準の安全性を保証するものになっている。

任意の認定制度は、ドイツの 97 年デジタル署名法により導入され運用されているセキュリティ水準をオプションとして、存続・維持させる可能性を開いたものであるが、これは特にドイツからの要求に基づき指令に組み込まれたとされている。

(4)　署名指令におけるタイムスタンプ関連の言及

署名指令においては、ドイツのデジタル署名法と異なり、明確にタイムスタンプに言及する規定は含まれていないが、次のように、タイムスタンプを想定して言及している箇所がある。

まず、指令本文に先立つ考慮事項（立法趣旨にあたる）の中に次の規定が含まれる。

考慮事項「(9)　電子署名が極めてさまざまな環境および応用の中で、したがって電子署名に関するかまたはそれを用いるさまざまな新サービスおよび製品の中で用いられるであろうこと、かかる製品およびサービスの定義が証明証の発行および管理に限定されるべきものではなく、電子署名を用いたまたはそれに補助的なその他のサービスおよび製品、電子署名に関わる登録サービス、タイムスタンプサービス、ディレクトリサービス、コンピューティングサービスまたは相談サービスをも含むべきであること、」

これは、電子署名に関連して、タイムスタンプサービスが供給され、利用されることを予定していることを示すものであろう。

また、「付属書Ⅱ　適格証明証を発行する認証サービスプロバイダの要求事項」の中には、「(c)　証明証が発行されまたは取り消される日時が精確に決定され得ることを確保すること。」という規定が含まれている。この規定は、証明書の発行や取消(失効)に関わり、正確な日時の確定が求められることを定めたものであるが、この要求を満たすためには、タイムスタンプの利用が不可欠であるとの説明がみられる。後述のドイツ・新電子署名法の立法理由の中でタイムスタンプの規定を定めているのは、指令のこの条項を実施するために不可欠であるからであるとの説明[12] がなされている。

ダの要求事項」は適格証明書を発行する認証機関・認証サービスプロバイダの要件を定め、その事業者としての信頼性、セキュリティ条件、システム、製品等について規定し、付属書３「安全署名作成装置(ユニット)の要求事項」は、エンドユーザーに信頼性のある署名をさせるために必要な署名作成ユニットについて定めている。付属書４「安全署名検証についての推奨事項」は、適格電子署名の必要的な要求事項とはされていない。

[12] Georg M. Bröhl/Alexander Tettenborn, Das neue Recht der elektronischen Signaturen, 2001, S. 57.

４．１．３　ドイツにおける新電子署名法－電子署名大綱法－とその後の展開

(1)　EU 電子署名指令への対応・新電子署名法等の制定

ドイツでは、こうした指令の内容を実施するために、「電子署名大綱法およびその他の規定改正法[13]」の第一条によって前述のデジタル署名法を廃止し、電子署名大綱法(署名法 SigG)[14] を定め、従前の免許制により免許を得ていた認証事業者と同等の要件を満たすものについては、任意の認定制度を導入して現在に至っている。同法は、これらと同等の水準にある(主張された安全性)ものを適格電子署名(qualifizierte elektronische Signatur)として限定し、その基礎となる認証機関に届出義務(４条)を課すとともに、各種の義務を課して、安全な署名の実現のための基盤整備をしている。旧デジタル署名法により免許を与えて実現していた程度の安全性の水準にある認証事業者は、新法により認定を受けた事業者と同等の扱いとしている。そのことから分かるように、旧デジタル署名法で実現されたものとほぼ同等の内容が新法の認定制度により実現されているといってよい。新法では、認定を受けた認証機関には、いわば「包括的に検査された技術上および運営上のセキュリティ」が確保されていることを示し「優良証」を与えるというサービス・モデルの考え方にたっているとされる。署名法上は、(認証サービス)「プロバイダ認定を伴う適格電子署名」(署名法１５条１項)という用語が用いられている。

新署名法では、EU 電子署名指令に対応した用語への置換えを行っているほか、指令の定める 4 つの電子署名の種類(3 つの電子署名の段階と付加的要件をみたす電子署名)を署名法の中に位置づけ、第３段階の署名については、「適格電子署名」としている。また、旧法では、法令に基づき技術的な要件を定めていたのに対して、新法では、EU で制定された技術標準を参照することにより、EU 域内での認証サービスプロバイダ(認証機関)(署名法４上)およびそこで用いられる技術的コンポーネント(署名法１７条)の水準を確保することにしている。

また従前おかれていなかった署名の効力や訴訟上の取り扱いについての規定は、いわゆる形式規定適合化法「現代的な法的取引への、私法上の形式規定およびその他の法令の適合化のための法律」[15] によってもうけられることとなった。[16] この改正により、

---

[13] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften v. 16. 5. 2001 (BGBl. I S. 876).新署名法については、Alexander Roßnagel, Auf dem Weg zu neuen Signaturregelungen - Die Novellierungsentwürfe für SigG, BGB und ZPO -, MMR 2000, S. 451 ff.; ders., Das neue Recht elektronischer Signaturen - Neufassung, des Signaturgesetzes und Änderung des BGB und der ZPO -, NJW 2001, S. 1817 ff.; ders., Das neue Signaturgesetz - Grundlage des elektronischen Rechtsverkehrs, MMR 2001, S. 201f.など参照。

[14] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG). 拙訳「ドイツ新電子署名法」立命館法学 279 号 163 頁以下(2002 年)参照。署名令も新たに制定された。Verordnung zur elektronischen Signatur Signaturverordnung (SigV) v. 16. Nov. 2001 (BGBl I S. 3074).新署名令については、Alexander Roßnagel, Das neue Signaturverordnung, BB 2002, S. 261 ff.も参照。

[15] Gesetz zur Anpassung der Formschriften des Privatrechts und anderer Vorschriften an den modernenn Rechtsgeschäftsverkehr v. 13. Juli 2001, BGBl. I S. 1542.

[16] Susanne Hähnchen, Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr,　NJW 2001, S. 2831 など参照。

民法典の中で、電子署名法による適格電子署名を付した「電子的な形式(elektronische Form)」が新設され、従来の契約書等と同等の取り扱いが保証され(民法典 126a 条[17])、さらにまた訴訟上の一定の(表見証拠 Anscheinbeweis としての)証拠能力が与えられる(民事訴訟法 292a 条)こととなった。またこの改正に際し、民事訴訟法、行政裁判所法など各種訴訟法の改正によって、準備書面などの訴訟上の文書としても認められ、オンラインでの訴訟提起等のための基盤整備も同時に行われている。

(2) 新電子署名法上の電子署名の種類とその違い

ここで簡単にドイツの署名法による電子署名の違いについてみておこう。[18]電子署名指令を受けて、署名の効力や安全性の違いが重要となるからである。

① テキスト形式に際しての署名 ＝ 第１段階

民法典 126b 条で新たに法定されたテキスト形式(Textform)は、特定の署名技術を用いない方法での氏名の記載等による方法であり、なんら特別の法的規制もなく、署名の検証等も不可能である。法律上、テキスト形式でもよいとされるものがある。

署名法上は、「単純署名(Einfache Signatur)」(署名法２条１号)にあたり、データ保護の規定のみが適用される。

② 先進電子署名(Fortgeschrittene elektronische Signatur) ＝ 第２段階

なんらかの電子署名技術を利用して、署名者の本人確認とデータの完全性の確認を可能とする条件をみたすものが先進電子署名である(署名法２条２号参照)。電子署名の中では、もっとも安全性が低く、また法的規制もほとんどなく、一方で、何ら特別の法的効果も与えられていない。また PKI も必要としない。

③ 適格電子署名(Qualifizierte elektronische Signatur) ＝ 第３段階

先進電子署名のうち、作成時点で有効な適格証明証に基づいており、かつ(チップカードなどを用いた)安全署名作成装置(ユニット)により作成されたものをいう(署名法２条３号)。この適格証明証とは、署名法４条ないし１４条で定められた要件をみたす(と主張する)認証機関が作成した電子証明証のことをいい、次に述べる認定を通じて事前に審査はされていないが、署名法により届出制に服する認証機関が発行するものである。

適格電子署名は、法的には文書形式を代替するものとして実体法上認められ(民法典

---

[17] 民法典 126a 条「(1) 法律上定められた文書形式が電子的形式により代替されるべきときは、意思表示の作成者(Aussteller)は、これにその名前を付加しかつ署名法による適格電子署名を付さなければならない。
(2) 契約に際しては、当事者は、それぞれ同内容の文書に、前項で示された方法で電子的に署名しなければならない。」

[18] 各種の署名手続の違いについては、さしあたり、Alexander Roßnagel, Rechtliche Unterschiede von Signaturverfahren, MMR 2002, S. 215 ff.; ders., Die elektronische Signatur in der öffentlichen Verwaltung: Hoffnung und Herausforderungen, in: ders. (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung, 2002, S. 13 ff.参照。

126a 条など)、訴訟法上も、表見証拠としての効果を与えられているが、訴訟上は、認証機関が事前に行政的審査を受けていないために、当該署名が適格署名に該当すること、署名法による検証が可能なことを個別に、事後的に証明しなければならない。また署名法上は、適格署名についての届出認証サービスプロバイダについては、5 年間の文書保存が義務づけられ、また同じく 5 年の署名検証を可能にすることが義務づけられている結果、証明証の有効期間(5 年)に加えて 5 年間のみ、署名の検証(つまり本人確認と完全性確認)が可能である。

「適格タイムスタンプ」は、この適格電子署名に関わる証明書の発行のための技術的・組織的・人的要件とほぼ同様の要件をみたすタイムスタンプである。

④ 認定認証サービスプロバイダの証明書を利用した電子署名 ＝ 付加的要件

認定を受けた認証サービスプロバイダにより発行される証明証を利用して、さらに署名法で定められた署名作成装置(ユニット)によりなされる適格電子署名は、もっとも安全性が高く、また長期的に検証可能な電子署名である(かりに「認定電子署名」という)。認定電子署名は、認証機関が技術的にもまた人的および組織的にも業務運営上もその安全性が事前に審査され(証明された安全性)、監督庁たる郵電規制庁の根幹認証に基づく署名を用いて証明証が発行される。文書形式の代替が法的に認められるほか、事前に証明された安全性を援用することによる証明も容易であり、また署名法上、証明証が失効した年から 30 年間の文書保存および検証可能性が義務づけられているので(署名令４条２項)、証明書の有効期間後 30 年間は、署名の検証が保証されている[19]。

(3) 新署名法とタイムスタンプ

新署名法は、タイムスタンプについては、旧法が認証機関の義務的なサービスとしていたのと比べて、任意のサービスとして位置付けているが、この点は、電子署名指令との適合性に配慮したものだとされている。新署名法上は、適格電子署名と同様の技術的および人的な要件でセキュリティを確保して生成・供給されるものを「適格タイムスタンプ」として区別し、適格タイムスタンプを提供するための要求事項(署名法５条５項)を、適格電子証明書を発行する場合に準じて求めている(署名法９条)。また新法は、技術中立的に規定をしているとされ、具体的には、署名なしでのタイムスタンプの提供が可能になっている(署名法９条参照)。

新署名令も、新署名法にあわせて制定された。その中では、タイムスタンプに言及する規定は、整理されたが、署名済みデータの長期保存に関する規定は、若干の表現を変えながら存続している。(後掲・資料参照)

[19] 認証事業者の破産や事業中止の場合も、他の事業者または郵電規制庁に業務および文書等が引き継がれることにより、署名の長期的な検証可能性が保証される。

４．１．４　ドイツにおける署名法による PKI の現状

ドイツにおいては、これまでみてきたような電子署名を支える認証サービスのシステム、いわゆる PKI(Public Key Infrastructure)は、民間中心で構築されてきている。これまで、旧署名法による免許[20] または新署名法による認定を受けた事業者(認証機関、Certification Authority; CA)の数は、2003 年 1 月末の段階で、22 事業者、また署名法による届出をした事業者が１事業者となっていたが、調査を行った 2004 年 3 月末時点では、27 事業者となり拡大してきている(届出事業者も認定を受け、適格電子署名の認証業務を行う認証機関はすべて認定認証事業者となっている)。[21]

認定認証機関の中には、自ら設備を有して認証サービスを提供する認証機関と、他の認証機関に委託して自らの名前で認証サービスを提供する認証機関(バーチャル CA)とがある。電子署名法による（任意）認定を受けた認証事業者については、電子署名についての全体的な監督権限および認定権限を有する電気通信郵便規制庁(郵電規制庁)が根幹認証機関(Root-CA)として署名キーの認証を行い、そのもとに 2 段階的な PKI の構造で構築されている。

ドイツで認定認証業務を提供している認証機関どうしの間では、ブリッジ認証局を解した証明書の検証のしくみがとられてこなかったので、異なる認証事業者の証明書の検証をどのように確保し、相互運用性を保証するかが重要な課題になってきた。認定認証機関相互間では、その相互運用性を確保するための標準化へ向けた努力が続けられてきており、このところ開発されてきた規格(ISIS-MTT)によって、相互の電子署名検証を保証するしくみができあがっていくことになっているとされている。

ドイツでは、行政手続の相手方である民間部門での PKI は、法人が用いる電子署名[22] も含めて民間の認証機関により構築され、行政手続の上でも、民間の認証サービスを利用することとされているほか、行政機関の側のいわゆる組織認証基盤についても、ドイツにおいては、行政機関側の証明証は民間の認証機関から調達するものとされている。[23][24]その

---

[20] Wendelin Bieser, Signaturgesetz: Die igitale Signatur im europäischen und internationalen Kontext - 1. Teil, RDV 2000, S. 197 ff.; 2. Teil, RDV 2000, S. 264 ff., 200; Volker Zeuner, Erfahrungen mit der Umsetzung des deutschen Signaturgesetzes, in: Ivo Geis (Hrsg.), Die digitale Signatur - eine Sicherheitstechnik für die Informationsgesellschaft - Ein Leitfaden für Anwender und Entscheider -, 2000, S. 51 ff.は、旧署名法施行後の普及の遅れなどの状況をまとめている。旧署名法下の免許 CA は、９CA であるが、そのうち、Produktzentrum TeleSec der Deutschen Telekom AG、Deutsche Post Signtrust、DATEV eG の３CA を除く、各地の税理士会ＣＡなどは、ヴァーチャルＣＡである。ドイツ公証人連合会も、連邦全域の公証人ネットのために「ヴァーチャル認証機関」を設立し、自らの名前で、自らの登録機関 Registrierstellen によって、しかしドイツポスト系サイントラスト社のチップカードおよびトラストセンターを利用することによるサービス提供を開始している。

[21] 郵電規制庁のサイト(http://www.regtp.de/tech_reg_tele/start/in_06-02-04-00-00_m/index.html)で、事業者名、免許・認定年月日等が公表されている。なお、１事業者は、業務を休止し、認定を取り消されているが、同社が発行した証明書等については、郵電規制庁に引き継がれている。

[22] ドイツの署名法上は、署名キーは、自然人にのみ帰属することが予定されているために、法人の利用する署名も、担当者たる職員・社員が法人の仮名を利用して署名をすることとされている。仮名の証明書は、こうした法人や、行政機関などの署名を実現するためにも利用されている。

[23] 連邦政府は、2002 年 1 月 16 日の決定(Beschluss der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung v. 16. Jan. 2002)の中で、適

際、職員の属性認証のための本人確認と登録は行政機関で担当し、電子証明書の発行・登録・管理などの認証サービスの提供は、民間の認証サービスプロバイダを利用するヴァーチャル CA のしくみが特徴的である。そこでは、職員の登録は、行政機関側で行うが、職員が職務上用いる証明証は民間 CA から調達して、利用するという構造がとられることが多い。

こうしたドイツにおける PKI の利用方式は、行政側 PKI を直接行政により構築するのでなく、民間との協働により構築する方式によっているという特徴がある。

４．１．５　署名法後の電子署名関連法制の展開

これまでみてきたような一般法および私法分野で整備されてきた電子署名法制は、その後さらに各種電子署名関連法の分野でも法整備が進められてきた。以下、概観しておこう。

(1)　委託発注令改正

ドイツにおいては、公共調達に関する法制度(委託発注法 Vergaberecht)は、伝統的に私法上の契約によるとされてきたために、行政手続法の適用を受けない私法契約による公共調達が実施されてきている。[25]したがって、私法上の契約締結に至る公共調達手続は、一般的な行政手続法による改正の対象外となっているが、電子化の改革では、後述する行政手続法改革に先行した。前述のように、公共調達は、ドイツにおいても電子政府の重要な分野とされてきたが、法制度上も、電子調達を可能とするための法整備が他分野に先駆けて実施された。具体的には、まず、公共調達の内部的な準則および約款としての性格をもつ請負規程(Verdingungsordnung)のうち建設工事請負規程(VOB)が、97 年の EC 指令にあわせて改正され、当時のデジタル署名法によるデジタル署名を付しての申込などの電子的委託手続の基礎が作られた。[26]建設工事請負規程２１条１項１号では、「申込は、文書で提出しかつ署名がなされていなければならない。委託者は、それと並んで、署名法の意味のデジタル署名を付されたデジタル申込を許容することができ、それは暗号化されて提出されなければならない。……（中略）……」として電子化を認めることとした。その後、さらに 2001 年に改正された公共調達の手続を定める

格署名の証明証および装備は、民間から調達すると述べている。

[24] 州の例では、ニーダーザクセン州が、2000 年初頭に、予算会計制度に関与する約 12,000 人の職員に対して、ドイツテレコム株式会社のチップカードを装備させ、デジタル署名付の電子的な形式で全州の財政を管理している。Bieser, a.a.O., S. 200

[25] 拙稿「政府契約締結の争訟的統制―ＥＣ法によるドイツ公共調達法の新展開を中心に―」鹿法 31 巻 1 号 1 頁以下、6 頁(1995 年)。なお、ドイツの委託発注法は、本稿でも紹介した電子調達に関して関心を集めているだけでなく、委託先決定行為を裁判所で争わせる改革をしたことにより、かなりの実務上および理論上の展開を見せている。この点は、わが国の行政訴訟制度改革との関係でも興味深い素材を提供している。拙稿「ドイツ公共調達法と司法審査の保障－委託発注法改正法による裁判的統制の展開－」立命館法学 261 号 22 頁以下(1999 年)、同「ドイツ競争制限禁止法と公共調達－第 6 次改正による委託発注法の組込みとその後の状況－」公正取引 596 号(2000 年 6 月号)46 頁以下、同「公共調達に関する権利救済とその実効性―ドイツ委託発注法改正法後の状況―」立命館法学 271・272 号(下巻)1115 頁以下(2001 年)参照。

[26] Bieser, a.a.O., S. 201 も参照。

2001 年の「委託発注令」[27] においては、建設工事、物品調達、役務調達の全分野に適用される公共調達手続について、電子署名を利用した電子調達手続を承認した。

委託発注令１５条によれば、各調達規程に定めのないかぎり、郵便での文書による申込以外の方法も許容することができる旨定め、電子的調達手続についても、「デジタル申込には、署名法による適格電子署名を付しかつ暗号化するものとし、暗号化は申込のために定められた期限が経過するまでそれを維持するものとする」と定めることによって、メディアブレイクのない完全なオンラインでの調達の実施を可能とした。

(2) その他の行政分野での電子化対応

公共調達とならんで早期に電子化に対応したのが、膨大な事務処理が関わる社会保険関係の支払、会計処理手続である。このために連邦レベルでは、社会保険関係の支払、会計処理に、デジタル署名を用いることができるように改正を行った。1999 年に改正された「社会保険における支払手続、帳簿処理および会計処理に関する命令」[28] ７条３項は、当時のデジタル署名法によるデジタル署名を付した支払命令等の書類を認め、詳細は、1999 年 8 月に改正された「社会保険会計制度に関する行政規則」４１条[29] で定められることとなった。

また税法の分野でも、2000 年 10 月に改正された売上税法１４条[30] が、デジタル署名を付された電子的計算書を計算書として承認し、連邦財務省は、電子計算書の検証可能性についての通達「デジタル書類のデータアクセスおよび検証可能性についての諸原則 (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen(GDPdU))」[31] を 2001 年 7 月に発している。この対応により、e-billing が可能になり、電子署名を利用した、会計処理、帳簿処理を行うための基礎が作られた。これにより民間での電子商取引に対応した税法上の対応も開始されたことになる。

州レベルの立法としては、前述の Media@Komm プロジェクトに参加したブレーメン州が、1999 年 6 月 1 日の「行政でのデジタル署名の実証試験のためのブレーメン法」[32]

---

[27] Verordnung über die Vergabe öffentlicher Aufträge - Vergabeverordnung VgV v. 9. Jan. 2001, BGBl. I S. 110. 電子的契約を電子的形式として許容したいわゆる私法上の形式規定適合化法が基礎となっている。

[28] Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung Sozialversicherungs-Rechnungsverordnung SVRV, idV. v. 15. Juli 1999, BGBl. I S. 1627.

[29] Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV) in der geänderten Fassung vom 15. Juli 1999, Beil. zum BAnz. v. 6. Aug. 1999, Nr. 145a, S. 1 ff.

[30] Gesetz zur Senkung der Steuersätze und zur Reform der Unternehmenbesteuerung (Steuersenkungsgesetz - StSenkG) v. 23. Okt. 2000, BGBl. I S. 1433. 売上税法１４条４項を「署名法によるデジタル署名を付された電子的計算書も計算書として通用する。」と改正した。Oliver Sachtleben, Elektronische Rechnungen - Auswirkungen und Probleme des neuen § 14 Abs. 4 UstG, DB 2001, S. 614 ff.; Ralf Klapdor/ Dorrit Klapdor, Auswirkungen der Einführung elektronischer Rechnungen in das deutsche Umsatzsteuerrecht, DStR 2000, S. 2116 ff.参照。

[31] Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), idF v. 16. Juli 2001.

[32] Bremische Gesetz zur Erprobung der digitalen Signatur in der Verwaltung v. 1. 6. 1999, GBl. S.

で、また前述のバーデン・ヴュルテンベルク州「E 市民サービス法」も、実験的にデジタル署名を用いた行政手続の実証実験に法制度的に対応した。

(3) 各種訴訟法改正、送達法改正

前述した、私法上の形式規定適合化法は、私法上の法関係で電子的形式を法的に承認するとともに、各種の訴訟手続も電子的形式を利用して可能とする改正を行った。

それによれば、改正された民事訴訟法 130a 条(適合化法２条による改正)、労働裁判所法 46b 条(同 6b 条)、社会裁判所法 108a 条(同７条)、行政裁判所法 86a 条(同８条)、財務裁判所法 77a 条(同９条)などにより、訴訟法上も、各裁判所での電子的文書の処理に適合的であるかぎりで、準備書面等の訴訟手続上の文書の裁判所への提出も、適格電子署名を付した電子的文書を電子メール等で提出する方法によって認められることとなっている。

この民事訴訟法改正[33] に基づいて、連邦最高裁判所(Bundesgerichtshof; BGH)との訴訟手続を電子化するための命令[34] がすでに制定され、2001 年 11 月 30 日から施行されている。同命令の別表の中で、同裁判所に提出する際の電子化のフォーマットや手続等の細目が定められている。

さらに、訴訟手続の電子化にかかわっては、各種訴訟手続や行政手続等に関わる送達手続の改革も行われており(送達改革法[35])、その中で、電子的な送達による方法の選択も認められている。2002 年 7 月 1 日からは、この方法による正式の送達手続も(選択的に)電子的に実施されている。[36]

こうした法改正により、訴訟手続も電子化への対応を行ったことになる。今後、それぞれの裁判管轄毎に、電子化に必要な細目を法制化して、電子的訴訟手続の推進を行うことになっている。[37]

---

138 f.

[33] Christian Dästner, Neue Formvorschriften im Prozeßrecht, NJW 2001, S. 3469 ff.; Klaus Bacher, Eingang von E-Mail-Sendungen bei Gericht, MDR 2002, S. 669 ff.; Ingo Fritsche, Die Einführung des elektronischen Rechtsverkehrs im Privatrecht - Eine Übersicht, NJ 2002, S. 169 ff.; Wolfram Viefhues, Elektronischer Rechtsverkehr - rechtliche Aspekte und organisatorische Auswirkungen, CR 2001, S. 556 ff.電子文書の民事訴訟における証明の問題については、Stephanie Fischer-Dieskau u. a., Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, S. 709 ff.

[34] Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof - Elektronische Rechtsverkehrsverordnung – ERVVOBGH v. 26. Nov. 2001 (BGBl. I S. 3225).

[35] Gesetz zur Reform des Verfahrens bei Zustellungen im gerichtlichen Verfahren (Zustellungsreformgesetz – ZustRG) v. 25. Juni 2001 (BGBl. I S. 1206).同改正法は、弁護士、公証人、裁判所執行官、税理士などの職業的な信頼性があるとされる者、行政庁、公法上の社団もしくは財団に対して、ならびに明示的に電子的文書の伝達に同意した手続参加者に対しても、送達を電子的文書により行うことを認めた(改正された民事訴訟法 174 条 3 項による)。また、同法により、労働裁判所法、社会裁判所法、行政裁判法、財務裁判法上の送達手続も、民事訴訟法の定める送達手続によることとされ、電子的な送達の途が開かれた。

[36] 送達手続の電子化については、Martin Häublein, Zustellungsrecht - Zustellung von Anwalt zu Anwalt nach der Reform, MDR 2002, S. 563; Burkhard Heß, Neues deutsches und europäisches Zustellungsrecht, NJW 2002, S. 2417 ff.

[37] ハンブルク財務裁判所のプロジェクトからはじまった、この間の電子的訴訟手続改革については、別

(4) 住民登録法制の改正－電子的住民登録、電子的住民情報照会制度の導入

ドイツにおいても、国民が行政に対して行う住民届出制度(Meldewesen)[38] についての負担軽減や IT 技術の利用は重要な政策課題であったが、連邦政府は、届出制度についての大綱法を改正して(「届出法大綱法およびその他の法律の改正に関する法律」[39])、IT 技術を利用した電子的な届出についての枠組を定めるとともに、こうした届出についての規制緩和措置として、引越しの際の転出届けの廃止や、住居の賃貸人が転出に際して届出に関与する手続の廃止などの改革を行った。この改正に基づいて、州法により電子的な転居届などの電子的届出が法的に認められるとともに[40]、届出済みのデータのオンラインでの閲覧についても、その法的根拠が整備された。そしてさらに届出されたデータを、旧住所地の管轄行政庁、その他の行政庁、EU 加盟国等および私的機関に伝達することも、一定の要件のもとで、オンラインで可能とされることとなった。

４．１．６　電子的行政手続法－行政手続法等改正法

(1) 概要

これまで見てきたような個別的な行政手続の電子化の後、いわゆる行政手続法を改正し、電子的行政手続を一般法上整備する立法がすでに成立している。「第３次行政手続法的規定改正法[41]」によって、行政手続法(VwVfG)、社会保障法典第１編(SGB I)、同第

稿で紹介を予定している。

[38] 住民届出(Meldewesen)は、わが国の住民基本台帳と同様の、基本的な住民登録の制度であり、これに基づいて、国民のさまざまな証明、本人確認、住所証明などがなされる。住民登録等の権限自体は、州の権限である。また、本文で述べた改正に際しても、わが国の住民基本台帳ネットワークのように、中央にデータを集約する改革はなされていない。

[39] Gesetz zur Änderung des Melderechtsrahmengesetzes und anderer Gesetze v. 25. März 2002 (BGBl. I S. 1186).

[40] 住民届出大綱法 11 条 6 項は、州法によりデータの転送による届出を認めることを承認し、その際の申請者の確認は、署名法による適格電子署名により行うことを定めている。届出済みデータの情報提供については、同 8 条 2 項が同様に電子的に行うことを承認した。

[41] Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften v. 21. Aug. 2002 (BGBl. I S. 2322).法案は、BT-Drucks. 14/9000 v. 13. 5. 2002. 電子的行政手続法についての提案等として、Alexander Roßnagel, Die digitale Signatur in der |ffentlichen Verwaltung, in: Kubicek u. a. (Hrsg.), a.a.O., S. 158 ff.; ders., Die elektronische Signatur im Verwaltungsrecht - Modernisierung des VwVfG und des VwZG -, DÖV 2001, S. 221 ff.; Martin Eifert, Editorial Digitale Signaturen in der Verwaltung, K&R 2000, Beil. 2, S. 1(および同誌所収の各論文); ders./Lutz Schreiber, Elektronische Signatur und der Zugang zur Verwaltung, Die Folgen der EU-Signaturrichtlinie f}r die Verwaltungsrecht und die Verwaltungspraxis, MMR 2000, S. 340 ff.この行政手続法改正については、Hans-Josef Rosenbach, Erläuterungen und Anmerkungen zum Entwurf eines Gesetzes zur Änderung des Verwaltungsverfahrensgesetzes – Stand: Magdeburger Fassung, 24. November 2000-, DVBl. 2001, S. 332 ff.; Andreas Cartrein, Anmerkungen zum Entwurf eines Gesetzes zur Änderung der Verwaltungsverfahrensgesetze des Bundes und der Länder, NVwZ 2001, S. 413 f.; Arne Schlatmann, Anmerkungen zum Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften, DVBl. 2002, S. 1005 ff.; Heribert Schmitz/ Arne Schlatmann, Digitale Verwaltung? - Das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften, NVwZ 2002, S. 1281 ff.; Volker Ibisch, Der elektronische Verwaltungsakt - ein neuer Dokumententyp im Verwaltungsverfahrensgesetz, Jur-PC 2001, Web-Dok 210/2001 など参照。

１０編(SGB X)および公課法(Abgabenordnung)ならびに 64 の個別法令、合計 68 法令が改正された。

改正法は、行政手続に関する一般法である連邦行政手続法、社会保障法典および公課法の規定につき、電子的コミュニケーションについての規定を新設し、電子的な手続を一般的に認めるとともに、個別の法令で定められた手続毎に、長期にわたり検証可能な電子署名についての特則を認めるなどの法改正を行った。

その際の基本的な考え方は、以下のとおりである。

改正は、市民と行政との間での、法的に拘束的な電子的コミュニケーションの実現を目標としており、そのための行政手続規定の改正を行うものである。この改正では、先立って行われた私法規定における形式規定の適合化と同様、署名法に基づく適格電子署名を基礎として、行政手続における法的に拘束的なコミュニケーションを可能にすることを主旨としている。そのために、市民にとっては行政への容易なアクセスの確保と、行政にとっては電子的行政活動のセキュリティ(Sicherheit)と継続性(Dauerhaftigkeit)の担保が求められる。[42]

もともと行政手続法上は、手続の非様式性(Nichtförmlichkeit)の原則、形式自由の原則を採用しているので(行政手続法１０条、社会保障法典１０編９条)、すでに改正前においても電子的行政手続が認められるはずであったが、多くの個別法令が文書要件または署名要件によって、不様式性の原則を制限している。そこで、今回の改正で、一般条項により、電子文書についてもこうした例外的な文書要件等を充足させるよう定める必要があった。特に、オープンなネットワークであるインターネット上で伝送される電子的文書については、通例、通信相手の電子的な真正性確保(Authentifizierung)と伝送されたデータの完全性(Integrität)審査を保障するセキュリティ確保のための法的枠組みが必要となる。そのために署名法により実現された適格電子署名の技術および制度を、行政手続法上も利用することとした。その際、署名法等についても問題となった、EU 電子署名指令[43] の要件との適合性を図りつつ、さらに必要な範囲においては、行政手続の個別の特性から特に必要となる付加的な加重要件を個別に求める余地(署名法１条３項[44])を利用しようとしている。

---

[42] Begründung, BT-Drucks. 14/9000, S. 1.

[43] Richtlinie 1999/93/EG, a.a.O.

[44] 署名指令 3 条 7 項により認められた、公共部門における電子署名に対する付加的要件の承認によっている。

(2) 改正の基本方針

具体的な改正の基本方針は、次のとおりである。[45]

第一に、手続法に、文書形式と、適格電子署名を付した電子的形式との同等性を認める一般条項を定める。これは、私法上の形式規定適合化法でとられた、私法分野での電子的適合化の方針と同様である。これが、行政手続の全分野に適用される一般原則となる。適格電子署名は、手書署名が付された文書よりもより高度の、改竄、偽造等に対するセキュリティ水準を実現している。これにより、文書の原本が持つ、完全性、真正性、署名者の本人確認などの機能を同等以上に確保しようとすることになる。[46]

第二に、法令上、文書形式によることを求められている行政行為については、より高度の付加的な要件を課すこととした。すなわち、文書による行政行為は、長期にわたって、さまざまな公私の活動に法的な影響を与えることなどから、文書によることを求められているものであると考えられ、そのために電子的な形式の場合も、長期にわたって検証可能な電子的形式である必要がある。そこで改正法は、付加的要件として「永続的な検証可能性(dauerhafte Überprüfbarkeit)」を課すことを認めている。この要件は、署名法による認定を受けた認証サービスプロバイダが発行し、長期にわたって(最長で35 年間)検証可能な証明証に基づく適格電子署名によることを意味している。文書を代替する電子的形式の行政行為は、こうして、最長で 35 年間は、その真正性や完全性が客観的に検証可能に保たれることになる。[47]

なお立法理由では、文書形式による行政行為の場合でも、給付行政におけるそれのよ

---

[45] 以下は、提案理由の総論的部分(Begründung, BT-Drucks., a.a.O., S. 26 ff.)による。

[46] これは、適格電子署名という厳格な技術的・組織的要件の認証機関による証明書をともなう電子署名形式についてのみいえることに注意が必要である。また、ドイツの電子署名法上は、属性証明書による属性認証(署名法 5 条 2 項、7 条)により法人の機関や行政機関の特定の権限の担当者たる資格の証明がなされることが法制度上予定されており、また適格タイムスタンプ(時刻証明)サービスを利用することによる(同 2 条 14 号、9 条)、文書作成時の法的な確定も(法制度上の根拠を伴って)可能となっている。またドイツ署名法上は、仮名(Pseudonym)を証明証にとりこむことにより仮名による電子署名が認められているが(同 5 条 3 項、7 条 1 項、14 条 2 項)、これにより法人の機関による電子署名が可能なほか(わが国の法人登録に基づく法人認証とは異なる)、仮名を用いて個人情報を秘匿しながら法的に拘束的な意思表示をすることが可能となっている(仮名による個人情報の秘匿、防衛)。仮名を用いた署名は、EU の電子署名指令上も、明示的に認められる重要な考え方になっている(電子署名指令提案理由 25、指令 8 条 3 項、付属書Ⅰ(c)、Ⅳ(f))。いわゆるテレサービス(テレサービス法)の利用に際して、仮名を利用することは、ドイツでは、基本原則とされている(テレサービス法 4 条 6 および 7 項など)。仮名を利用する場合も、認証機関において厳格な本人確認がなされ、その情報が確保されることにより、法的な責任の追求の可能性は保たれる。仮名の利用による個人情報保護の考え方については、さしあたり、アレクサンダー・ロスナゲル(拙訳)「データ保護の新たな構想―インターネットの挑戦―」立命館法学 270 号 186 頁以下、190 頁以下(2000 年)参照。仮名による署名のうち、本人特定を困難とする仮名の利用は、後述のように、行政手続上は認められない。

[47] ドイツ電子署名法上は、最高水準の認定電子署名については、認証サービス事業者が破産した場合でも監督行政庁である誘電規制庁にそのデータおよび文書は引き継がれて、最長で 35 年もの長期にわたり検証が可能な状態が確保される。もちろんこの場合において、期間の経過により、署名自体の安全性が低下する場合に備えて、法令上は、再度署名を繰り返すなどの措置をとることが求められている(署名令 17 条による再署名手続)。

うに、給付がなされるなどの法関係の精算により短期間でその役割が終わるものについては、適格電子署名を付した電子的文書で足りるとしている。また申請など市民側について文書要件を課している場合も、一般条項により、適格電子署名を付した電子的文書で代替させることとしている。

第三に、こうした文書形式を代替するほどの必要性がない場合には、テキスト形式や先進電子署名を用いた電子的文書も用いる余地が認められ、その場合には、「電子的な(elektronisch)」(電子的に)という用語が用いられる(例、行政手続法26条1項2段2号)。この場合の「電子的な」は、電子的な文書を用いる場合の上位概念として用いられている。

第四に、こうした電子的なコミュニケーションが認められる場合を、公私双方の電子化の状況に対応して、限定している。少なくとも現状では、行政側私人側の双方で、電子化への対応は進んでおらず、電子的なコミュニケーションの用意がなされていない場合もあるため、手続法は、公私のいずれか受信者側が、電子的文書のアクセスルートを開き、そのルートからのアクセスを明示または黙示に認めている場合[48] に限定して、電子的コミュニケーションを認めるという考え方を採用している。このことは至極当然のことのように思われるが、立法理由によれば、こうした限定規定をおくことにより、電子的コミュニケーションへと「強制」されることに歯止めをかけているとしている。

第五に、現状で、行政実務上、電子的な文書と紙の文書とが混在し、あるいはその相互間で変換が行われる(特に、電子文書をプリントアウトして処理する)必要性に対応した規定を置くこととしている。つまり、適格電子署名を付した電子的文書は、電子的メディアに保存され、署名検証キーおよび証明書を利用して検証可能な限りでのみ、その有効性が認められることができる。電子的文書のプリントアウトは、検証不可能となるために、それだけでは電子的文書に対応する法的価値を失ってしまう。手続法改正では、プリントアウトされた電子的文書に、再び一定の証明を行うことによって法的価値を与える対応をしている。こうした証明なしには、プリントアウトされたものは電子的行政行為の内容の証拠となる手がかり(Beweiszeichen)でしかないのである。

改正法は、以上のような改正の基本方針に基づいて行政手続についての基本法を改正するとともに、行政手続に関する個別法も、全体的な見直しを行った。

(3) 連邦行政手続法の改正内容

以下では、改正の基本となる行政手続法の改正内容を中心に、検討しておこう。

連邦行政手続法は、次のような主要な改正が行われた。

① 第3a条電子的コミュニケーション規定の追加

---

[48] 立法理由によれば、行政側および法人や事業者のように業務として電子メールアドレスを掲げている場合は、黙示的に電子メールによるアクセスを認めているとし、一方で一般市民の場合、メールアドレスを掲げるだけではそうしたアクセスを認めているとは現状ではみれないとして、明示的にメールによるアクセスを認めることが必要であるとの解釈を示している。BT-Drucks., a.a.O., S. .

「〔電子的コミュニケーション〕

3a 条　電子的文書の伝送は、受信者がそのためにアクセス(Zugang)を認めている限りで許される。

(2)法令により命ぜられた文書形式は、法令による異なる定めのない限り、適格電子署名を付した電子的形式でこれを代替することができる。この場合においては、電子的文書には署名法による適格電子署名を付するものとする。署名キー所持者(Signaturschlüsselinhaber)の本人確認を可能としない仮名を用いた署名は、許されない。

(3)行政庁は、伝送された電子的文書がその処理に適合的でないときは、行政庁で利用されている技術的基本条件を示して遅滞なく送信者にこの点を通知しなければならない。受信者が、行政庁に対して、それが伝送した電子文書を処理することができないことを主張するときは、行政庁は、受信者に対しそれを新たな適切な電子的フォーマットでかまたは書類(Schriftstück)として送付しなければならない。」

この電子的コミュニケーションの承認規定においては、受信者が電子メールアドレスなどの明示または黙示の利用承認によって、コミュニケーションのルートを開き認めているかぎりで、電子的なデータの送受信によるコミュニケーションを許容した。電子的文書は、利用するソフトウェアの条件により処理の可不可の違いが出てくることから、処理しえないフォーマットの場合の対応規定もおいている。そしてさらに、法令が文書形式を求めている場合でも、署名法による適格電子署名を付した電子的文書によって、文書形式を代替することを一般的に認めている。この適格署名を付した電子的文書による文書形式の代替を認めたことにより、文書作成から、行政手続さらには文書保存に至るまでのすべての過程で、メディアブレイクのない電子的なデータによる処理を可能にしたのである。この電子的コミュニケーションの承認規定は、行政行為のみならず、その他の公法上の行政活動についても適用されるものである。

行政庁との電子的コミュニケーションは、法令による文書形式の指定がなく、形式上自由でかつ本人特定、内容確認および証拠保全の必要性がない場合は、「電子的に(elektronisch)」行うことも認めており、この場合は、適格電子署名以外の、先進電子署名やテキスト形式の署名も認められることになっている。

② 電子的文書の到達に関するみなし規定

電子的コミュニケーションに関わっては、手続参加者の住所、居所および事務所が国内にない場合に、受領代理者の指定を求める条文(行政手続法１５条)の中で、その場合の文書の到達に関する推定規定を１５条２段で定め、「電子的に伝送された文書は、発信後 3 日目に到達したものとみなす」とし、さらに不着または 3 日後以後の時点での到着が確認されるときは、このみなし規定を適用しないこととした。

また、後述の電子的行政行為についても、行政行為の通知についての４１条２項を改正し、到達について、「電子的に伝達される行政行為は、発信後 3 日目に通知さ

れたものとみなす。行政行為が到達しなかったか、または遅れて到達したときは、前段の規定はこれを適用しない。疑わしき場合は、行政庁が行政行為の到達および到達の時点を証明しなければならない。」との規定をおいた。

発信後 3 日目の到達みなし規定は、郵便による行政行為の通知と同様の期間設定であり、さらに同様の法律上の推定であるとされている。したがって、瞬時に相手方のメールボックスに到達しさらに瞬時に相手方に当該電子的行政行為が通知されたとしても、効力が生じるのは、郵便による場合と同様、発信の日から 3 日後ということになる。

③ 証明(Beglaubigung)規定の改正

文書の証明については、電子的証明の承認と、印刷された電子文書の証明についての規定が導入された。そのために、行政手続法 33 条のかた見出しは、「文書の証明」と変更され、従来の第４項３号で定めていたデータ処理組織によりそのデータ記憶装置に記録されたデータをプリントアウトしたもの(印刷物)の証明についての規定に代えて、電子的文書についての規定が挿入された。そこでは、電子的文書のプリントアウト(印刷物)(４項３号)ならびに書類の複写のために作成された電子的文書および適格電子署名を付された当初の文書と異なる技術的フォーマットをとった電子的文書(同４号)の証明ができるように明示し、これら改正された電子的文書およびそのプリントアウトの証明について、次のような規定を置いた。

３３条「(5) 証明書き(Beglaubigungsvermerk)は、第３項第２段による記載[49] に加えて、次の各号の事項を含んでいなければならない。

1 適格電子署名を付された電子的文書のプリントアウト(印刷物)の証明の場合には、次の各号についての確認。

a) 署名検証により誰が署名の所持者として示されるか

b) 署名検証によりいつの時点で署名を行ったと示されるか、および

c) どのデータを伴ったどの証明証がこの署名の基礎とされたか

2 電子文書の証明の場合は、証明権限ある職員の氏名および証明を行う行政庁の表示。第３項第２段第４号による証明権限ある職員の署名および職印は、永続的に検証可能な適格電子署名によりこれを代替する。

適格電子署名を付された当初の文書と異なる技術的フォーマットを有した電子的文書を本項第１段第２号により証明するときは、証明書きには、当初文書についての本項第１段第１号による確認を含めなければならない。

(6)第４項により作成された文書は、それが証明されているかぎりで、証明された写しと同等のものである。」

[49] 写しについて証明がされる当該書類の正確な表示(1 号)、写しが提出された書類と一致する旨の確認(2 号)、もともとの書類が当該行政庁により作成されたものでなかった場合で、証明される写しが、その当該行政庁への提出のためだけに当該写しがとられたものであることの指示(3 号)、ならびに証明の場所、年月日、証明権限ある職員の署名および職印。

手続法上は、こうした対応で、電子的文書と紙文書との混在や、これら間の変換を行った場合の、文書としての機能を確保するための対応をしていることが注目される。

④　電子的行政行為についての規定の整備

行政行為の内容的な特定性と形式について定める手続法３７条は、次のように改正された。まず、行政行為の形式として、電子的行政行為を明示的に承認し(同条２項での「電子的」文言の追加)、口頭での行政行為の電子的な確認ならびに電子的行政行為の文書での確認の規定を追加した。第３項は、次のように改正され、第４項が追加された。

「(3)　文書によるまたは電子的な行政行為は、それを発する行政庁を認識させなければならず、かつ行政庁の長、その代表者またはその受託者の署名または氏名表示を含んでいなければならない。法令により文書形式によることが命じられている行政行為について電子的形式が用いられるときは、署名の基礎となる適格証明証または付属の適格属性証明証が、行政行為を発する行政庁を認識させなければならない。

(4)　行政行為については、第 3a 条第２項により必要な署名に関して、法令により、永続的な検証可能性を定めることができる。」

また、文書による行政行為に理由付記を求めてきた手続法３９条も、電子的行政行為、または電子的に確認される行政行為についても拡張され、理由付記が求められることになった。

さらに、６９条２項は、正式の(要式的な)行政手続を終結させる行政行為について、文書で発し、理由を付記し、さらにそれを送達するものとするとした第１段に続けて、電子的行政行為により第１段の行政行為を発する際に、「永続的に検証可能な適格電子署名を付するものとする」との第２段を挿入した。この規定は、手続法７４条１項により、計画確定手続にも適用されるものであるから、今後は、電子的に、永続的に検証可能な適格電子署名を付してなされる計画確定も認められることとなる。

さて、以上が、行政手続法改正の具体的な内容である。わが国の議論状況や法制度からみても、次の点は、特徴的な点として指摘することができる。

まず、行政手続で利用される電子署名は、一般法たる署名法に基づき提供される民間の認証サービスを利用するようにしている。ドイツでは、こうした対応をすることによって、電子政府化の施策が、民間レベルでも、電子商取引への電子署名の普及を後押しする機能を持っている。そのことによって、署名法による適格電子署名を実現する製品およびサービスの普及と、普及によるさらなる低価格化の実現を目指している。

次に、行政手続で利用される署名手続の水準は、署名法による適格電子署名を基礎としつつも、必要に応じて、30 年以上の検証が可能ないわゆる認定電子署名の利用を求めることとしている。ドイツにおいては、いわゆる認定電子署名については、

長期にわたって真正性および完全性が検証可能であることをすでに署名法レベルで確保しているが、その利用が個別的に求められることになった。この点については、最高レベルに統一するほうが、コストの点でも、安全性の点でも望ましいとする意見[50]が出されていたが、結局、適格署名を基礎とする原則になってしまっている。

電子署名は、デジタルデータのままで、なおかつオンラインでの検証可能性があってはじめて、真正性および完全性が可能となり、それを保証するのが、認証機関へのオンラインサービス提供義務および文書保存義務であること、それを長期にわたり確保することが、訴訟等で事後的に電子文書の検証を保証し、法治国家の実現に不可欠な法的安定性を実現することにつながることは、わが国の議論に対しても重要な意味を持つものと思われる。

第三に、電子政府化を進めても、過渡的に、場合によっては最終的にも、紙文書と電子文書とが混在したり、相互のメディア変換を要することを考慮すれば、それぞれのメディア変換に応じた、文書としての機能確保の措置は非常に重要である。前述した、証明の手続を利用した、行政手続法の対応は、わが国でも、今後メディア変換に対応した手続規定を考える場合に、参考となる考え方である。

[50] Roßnagel, a.a.O., S. 46 ff.は、大量の手続に焦点をあてて、統一的に認定署名を利用することを提唱していた。

５．訪問機関・企業報告

５．１　ドイツ郵電規制庁(マインツ)

● 訪問日程：2004 年 3 月 18 日　10:00～12:00

● 対応者：Dipl.ing. Jurgen Schwemmer（電子署名部署の責任者）
Dr.rer.nat. Petra Wohlmacher（認証技術関係）
Assessorin jur. KerstinA.Reschke（法律関係）

● 報告者：鳥山　裕史（独立行政法人通信総合研究所　電磁波計測部門タイムスタンププラットフォームグループ　グループリーダー）
谷川　嘉伸（株式会社日立製作所　システム開発研究所第７部研究員）

● 組織概要：
マインツオフィスにトラストセンター、認証機関がある。（ボンが本拠地）
マインツに、ルートＣＡを設置して運営しており、タイムスタンプについての情報交換とルートＣＡの視察を行った。

● 講演内容：
ドイツの適格署名（クォリファイド署名：qualifizierte Signatur)は、法令上手書き署名と同等に扱われる。紙は、３０でも５０年でもそのまま残るが、電子情報では情報の改ざんを防ぐ、予防対策が必須である。これには、「署名が行われた時刻」が重要な意味を持ち、適格署名（クォリファイド署名）には、「正確な時刻」によるタイムスタンプが必須である。
タイムスタンプの適用対象は、法によれば、二つ。
・ その当該行為が行われた法律的な時刻を証明

・ 電子アーカイブでのデータの長期保管上の利用。（暗号技術の危殆化に対応）

有効な暗号アルゴリズムは、ドイツの官報(Bundesnzeiger 公報)に掲載される。これを変更する場合は、ドイツ BSI（情報技術安全局）と学者が協議の上で行うことになっている。

有効なアルゴリズムが変更された場合に、それを自動的に反映する方法について検討を進めている。E-アーカイブシステムへの自動反映であるが、まだ実装はできていない。

〔1997 年 ドイツの電子署名法令制定〕

特に銀行取引などでは、オリジナルの署名との真正性、同一性を確かめることが重要であり、これが電子署名でないとスムーズにいかない、ということから、法令が作成された。これは、従来のものよりも高い技術的な要件であり、そのため、ヨーロッパの関係国は、驚きをもって受け止めた。特に、ＥＵは、欧州全域の統一的な法制をめざして、次のＥＵ指令を制定した。

〔1999 年 EU 電子署名に関する指令〕

ＥＵ指令は、結果的に、技術的な妥協でなく政治的な妥協になってしまった。その結果、数段階の署名の種類を定めることとなった。

その後、2001 年 5 月 ドイツの法令も、EU のガイドラインに基づき改正された。技術的な安全に対するニーズと要求事項は、1997 年のものを継承した。EU の各国の相互運用性を確保することが大きな問題である。

ドイツが 1997 年に導入した署名水準と同等のものを適格署名として、手書の署名の代替と認めることにして、一つの標準とした。この適格署名は、手書き署名と同等な署名である。

こうした、法令面の統一化と、それに伴う技術面の EU での統一化は、プロファイリングによって行うこととされている。標準としては、ドイツで開発された相互運用性確保のための標準である ISIS-MTT に準拠して行くこととしているが、今後ＥＵレベルでも追求してきたい。

署名のパラメータ自体は、もともとは相互互換性がないが、オプションセットからパラメータを選択することによって互換性を確保することができる。これをプロファイリングと呼んでいる。認定を受けたすべての認定認証機関で、共通の標準である ISIS-MTT を使うことで、ルートＣＡの稼動とともに互換性を確保することをテスト中である。

● 質疑応答：

Q: ISIS-MTT でどの認証局間で相互運用可能なのか？

A: まだ運用されていないが、ルートＣＡの施行準備の最終段階にあり、2 ヵ月後ぐらいには運用できる予定である。テストとして、動き出したところである。
ISIS-MTT は、認定認証機関相互間の証明書検証の相互運用性確保のための標準として策定されたものである。

Q: 日本ではブリッジ認証モデルを考えているが、ドイツでも検討されたか？

A: トップレベルで管理するのが容易であるため、ルート CA モデルを採用した。
ブリッジモデルでは、認証事業者が撤退したときに、引き継ぐのが難しい。ドイツでは引継ぎも法律の中に含めた。実際、認定認証機関のうちサービス停止したものが 1 社ある。
署名の効力は最終的には国が保証することになっているので、電子署名に関する署名の質の審査や監視も国が行うべきである。
ルート CA をやっているために、RCA が CA 証明書を発行したタイムスタンプ事業者が撤退しときにも、彼らの行為をフォローアップすることが可能であることに気づいた。
同様に、国際的に展開する認証サービス企業にも監視力をおよぼすことができる。スイスでタイムスタンプサービスを行うドイツ企業があるが、規制庁が、どのように監査するかについても、契約に盛り込まれている。RCA が発行する CA の署名証明書をコントロールすることで実効性が出てくることになる。

Q： 電子署名の要件が他国と比べて高いのは？

A： ドイツ民事訴訟法の真正性推定規定が原因である。署名の署名者本人への法的帰属性を重視したため、高い要件となっている。電子署名については国が責任を持つ。署名に使用するアルゴリズムは国が設定し、アルゴリズムの変更などについても、国が責任を持つ。この考えはヨーロッパ全体に広まっている。これはドイツのパスポートに問題があったときに、ドイツが責任を持つのと同様である。技術的な安全性の点でも、RCA のディレクトリやデータも二重化するなどして対応しており、攻撃がなされても、問題がないように責任がもたれている。

Q： 新しい暗号アルゴリズムが自動的にロードされる件、どのようにして？

A： 紙の形はドイツの官報。RegTP の Web サイトにも掲載。現在は手動でチェックしないといけないが、これが自動で行われるようにする計画である。

Q： 連邦政府や自治体では、認証システムはどのように利用されている？

A： これは、ネットワークのテーマであるが、電話システムと同じで、参加者がいないと意味がない。1997 年から大きな変化はないが、システムが完全に実現され相互運用性が高まれば、ある時期に爆発的に普及するのではないか。

現時点で、ドイツ全体で 3 万枚のクオリファイド証明書が発行されている。1～2 年後には 3000 万から 4000 万枚発行されることを予想している。ベルリンの連邦経済省で言及されるだろうが、Job カード(ジョブ・カード；職業安定カード)や、職員の ID カードなどの導入が検討されている。

最近設立された署名協議会(Signaturbündnis)のプロジェクトで、銀行カードに署名機能を組み込もうとしている。銀行カードが 8000 万枚流通しているが、現在のものは、適格署名には適さない種類のものである。最近のチップカードでは技術的に可能であり、これらも適格署名の対象にしていきたい。

Q： 長期保管に関する技術動向は？

A： いくつかのパイロットプロジェクトがある。たとえば、ArchiSig プロジェクト(代表者：カッセル大学アレクサンダー・ロスナゲル教授)では、1 ヵ月を 30 年として、タイムスタンプを押した保管書類を 30 年後に裁判の証拠として提出した場合を想定した、訴訟シミュレーションを行った。

認定署名（認定認証機関の発行した証明書を利用した署名）の場合にはなんら問題なかった。適格署名も問題なかったが、これには、認証プロバイダがまだ市場にいること等の条件が必要であった。

シンプル署名(先進署名)は口頭供述と同等レベルであった。報告書が出版される予定である（ドイツ語）。

ハイデルベルグ大学病院もプロジェクトに参加した。アプリケーションは、電子カルテの保管である。保管のためには、タイムスタンプが必要だということが証明されたことは、みなさんの関心からは重要でしょう。

Q： タイムスタンプの営業実績、利用頻度等に関する情報は？

A： タイムスタンプサービス業者は、複数ある。認定を受けたタイムスタンプに特化した事業者は 1 社であり、Authentidate 社だけである。TimeProof のサービスを利用している。

利用頻度についてはわからない。

Q： 証明書の値段は？

A： 署名令の別表に詳細な手数料の定めがある。認定の際に必要な認定手数料は、3500 ユーロである。CA に対する証明書は、500 ユーロである（25 認定認証機

関が証明書を受けている)。この値段に満足してはいない、中小企業には高すぎる(RegTP の経費を償うように手数料の設定をしているから)。

Q： 事業者がユーザーに出す証明の値段は？

A： 市場における証明書サービスはインフラサービスである。これまでは、こうしたインフラについてのビジネスモデルがなかった。例えば、クレジットカードにはコストがかかっているが、利用者は払っていない。インフラ上のアプリケーションサービスでビジネスすることを想定している。したがって、インフラの部分のマーケットや、ビジネスモデルについては語れない。今後さまざまなビジネス、アプリケーションに組み込まれて署名が普及していくことと思われる。

Q： クオリファイド署名には、クオリファイドタイムスタンプが必須か？

A： 1997 年の法律では、タイムスタンプは必須だったが、当初の認定認証機関のサービスでは実際的にはタイムスタンプを提供しなかった。97 年法制定当時には、タイムスタンプサービスを提供する事業者がなかったので、特に必須サービスとして法律に含めた。

現在の法律では義務的サービスとしては「タイムスタンプ」を含めていない。タイムスタンプ市場が出来たので、それに任せている。ドイツの経済大臣の方針である「出来る限り民間に任せる」という考え方に基づいている。

2001 の法改正では、認定認証局に対するタイムスタンプサービスの義務化はなくなったが、タイムスタンプの用語は削除されていない、あくまで、オプションサービス的な位置づけとなった。ただし、省令レベルの署名文書の長期保管に伴うタイムスタンプは必須のままである。

Q： タイムスタンプ付きの署名とローカル時刻の署名の差は？

A： タイムスタンプ付きの署名とローカル時刻の署名の差は、信用度である。

裁判時には、タイムスタンプの方が信憑性が高いはずである。認定を受けたタイムスタンプ事業者の信頼性が高くなるはずである。また、法の中でも時間の重要性が高い場合には、タイムスタンプを付するよう要求している。

時刻情報の信用性を低いものから順番に並べると、(1)計算機のローカル時刻、(2)普通のタイムスタンプサービス、(3)適格タイムスタンプ、(4)認定を受けた事業者のタイムスタンプサービス(例えば、Authentidate 社)という序列になろう。

タイムスタンプに適切なアプリケーションは、何かを行ったときの時間が重要なアプリケーションである。例えば、保険の申込、公募、入札、など、こういう場合には、タイムスタンプが重要になる。

Q： 認定を受けたタイムスタンプ局の時刻に関する要件は？

A： ドイツには「時間法(Zeitgesetz)」がある。UTC が基準である。ドイツ連邦物理技術庁が電波（長波）によって時刻情報を送っている。ドイツ国内では、ドイツ連邦物理技術庁のものを利用する。これに CA の時計を同期させる。

Q： 適格タイムスタンプ局の時計に関する要件は？

A： 1 秒以下などの精度に関する基準はない。「時刻の偽造可能性をなくしていること」が条件である。クオーツの時計と並べて。GCCF76510?

1997 の法律時は、タイムスタンプ局の要件が規定されたが、今はなくしている。97 年法にあわせて「措置カタログ(Massnahmekatalog)」を定めていたが、あまりにも厳格過ぎると懸念されたため、その後廃止している。

認定を行う際に、認証機関の技術的な要件を指定調査機関が調査し認定を行っているが、その検査・監査の時の確認書（要件に合致した時計を持っている）が、BSI、T-Ssystems、TÜViT など指定調査機関により発行されており、この認定証の中に具体的な技術仕様は叙述されている。監査レポートが送られる。この報告書は、RegTP の Web ページにも PDF で置かれている。

適格タイムスタンプの仕様はある。RFC などである。仕様をプロバイダが絶対に遵守する必要はない。仕様は、インターネットで公開されている。ドイツは技術にオープンである。技術(IT-Sec, CC など)が国際的にセキュアであることをチェックするだけである。

25 機関は、RegTP にサービス内容を申請する。RegTP が審査する。指定調査機関がそれだけのコンポーネントがあるのかなどをチェックする。

Authentidate 社は、あくまでも、一般の CA としてではなく、タイムスタンプサービスだけを申請した。他の機関もタイムスタンプサービスをしているはずである。

署名法第 2 条の 8 項を見ると、定義として、認証サービスプロバイダは、自然人か法人である。クオリファイド証明書かクオリファイドタイムスタンプを発行することができる。一つでもよいし、両者を発行してもよい。

Authentidate 社は、タイムスタンプサービスを含めたフルサービスの供給者として、市場に出ている。タイムスタンプと他から買ってきたサービス（e-mail やクオリファイド証明書）を組み合わせてサービスを提供している。

Q： EU 全体での取り組みは？

A： EU 指針を国内の法律として国内法化している。各国のレベルに違いがある。不完全なものもある。

10 月に EU 拡大。EU に新規参加する国は EU 指令をほとんどそのまま条文化し

たものを採用するはずである。しかし、それらを含めて EU 構成国間の相互運用はできないだろう。

EU 指針は 3 つの目標があった。(1)商品に対する市場開放、(2)技術不確定(技術にオープン)な表現、(3)ヨーロッパ全体の相互運用性確保。2 と 3 の要件は互いに相反する。これらの 3 つをハーモナイズすることが大きな課題である。技術の標準化については、ヨーロッパ規格委員会で技術を規格化する。

1997 年と 2001 年とドイツは二度の法制定を行ったが、EU レベルでは、次の、つまり第 3 の電子署名法制がありうる。立法と技術をつなぐものとして、RegTP の検査・監査・手続きが重要である。

共通な形での証明書、相互運用性確保のチェックを行う。これを行うために、2 年前に「FESA(Forum of European Supervisory Authorities)欧州監督機関フォーラム」というグループを発足した。ヨーロッパ全体の認証サービスプロバイダを監視するのかどうかを検討する。5〜6 回会合を持つ。

クロスボーダーの監督は、難しく、ドイツの C 会社が B 国で製品を作って、A 国で販売するような場合は、監査の目が届かない。各国の監査者との協力が重要である。

10 の新規 EU 加盟国(ハンガリー、チェコ、など）も参加している。数年後に形になることを予定している。この中で唯一ドイツは、統一的なインフラを作り上げている。

Q： 第 3 の電子署名法には個人認証は入るのか？

A： 州レベルで個人認証に取り組んでいるところもある。住民登録機関が、認証サービスを統合しようという意見もある。連邦の機関が、その他の機関のために、職員の認証サービス（行政 PKI）を構築しようとする意見もある。署名法は、オープンなので、その要件を満たせば、実現するものと考えている。

Q： Authentidate 社へは、装置、あるいは、法人に対して証明書を発行したのか？

A： 両方である。署名作成のスマートカードは、国際的な IT セキュリティを満たしているのかを確認した。RegTP の Web ページにチェックシートがある。仕事をするときのプロセス、建物、スタッフ、安全コンセプトを会社は提案しなければならない。

Q： 証明書の有効期限は？

A： 認定（証明書）（公開鍵証明書ではない）の有効期限はない。3 年に一度監査を行う。1997 年は国際的に通用するスペックをスタートとした。

シェルモデルを基にした。3 社がかかわる場合、1 つのパートナーが無効になる

と、全てが駄目になるというモデルである。1997 年当時は、シェルモデルしかなかった。有効期間は 3 年であった。クレジットカードなどの銀行カードの有効期限をそのまま採用した。

ただし、署名の場合、署名後、20～30～50 年後も過去有効であったのかどうかをチェックしなければならい、出来なければならない。現在は、チェーンモデルへ移行した。

認定認証機関の証明書は、4 年である。1 年中、Certification のための証明書を作れるようにするために、ルート証明書有効期限は 5 年である。アルゴリズムとしては 6 年間有効でなければならない。

法律にも数字が書かれているが、実際にはもう必要ないので、いつかはなくなる可能性もある。

何故問題が出てくるのかというと、ドイツの ID カードの有効期間は、10 年であり、証明書の最長 5 年の有効期限よりも長い。そこでこの問題の解決のためには、有効期限の制限をなくするか、この中へ長い鍵を入れることが必要である。5 年過ぎると、再度証明するようにすることも検討されるかもしれない。もちろん、10 年間保存できるチップも必要であるが、これは別問題である。

Q： 再署名の要件である「タイムスタンプを適用する」は、ドイツの署名法に含まれる。EU 指令には無い。EU 他国の動向は？

A： われわれには分からないが、この問題は、同様に他の国の場合にも出てくる問題である。タイムスタンプを含めることをドイツとして EU に働きかけている。実際、1997 年に行った。他国はこれにはしたがわない状態である。ただし、他国の中には、ドイツの署名法制に似てきたものもある。

ISIS-MTT、FESA といったワーキンググループ、EU コミッションの「９条グループ」、などで法的、技術的な規格を検討している。EU 全体のハーモナイズを試みている。

ロスナーゲル教授と検討しているが、次の法律改正では、署名とタイムスタンプの両方ではなく、タイムスタンプのみで規定する予定である。

現状のドイツの法律で言う「タイムスタンプ」は、サインとタイムスタンプを意味している。将来は、本人の署名の要素をなくし、タイムスタンプのみとする予定である（機械的な大量署名、大量タイムスタンプに対応するためと思われる）。5 年後は、サインは必要なくタイムスタンプだけになる。

Q： 延長された署名も国が責任を持つのか？

A： 100%保証するものではなく、有効なアルゴリズムを当時使っていたことを保証するのみであり、当該アルゴリズムを用いた署名が偽造不可能であったことの保

障にはなる。署名法によって、署名法の関係で BSI の場などで暗号アルゴリズムについて公に議論できるようになった。アルゴグループ（欧州全体）でアルゴリズムを検討している。

５．２　AuthentiDate 社（デュッセルドルフ）

● 訪問日程：2004 年 3 月 19 日（金）　10:00~12:20

● 場所：ドイツ　デュッセルドルフ　ニッコーデュッセルドルフホテル会議室

● 対応者：Jan.C.E.Wendenburg(CEO、写真左)
Dr.PercyDahm(Director IT/Development、写真中央)

● 報告者：遠藤　宏（株式会社 NTT データ　ビジネス開発事業本部
セキュリティビジネスユニット　ビジネスユニット長）
櫻井　徹（株式会社 NTT データ　技術開発本部　シニアエキスパート）

● ヒアリング内容：
会社紹介（Jan.C.E.Wendenburg）

AuthetiDate 社は、欧州、米国で活動している。米国では、NASDAQ に上場している。欧州（ドイツ）では、政府から認定されたタイムスタンプを発行している。米国には、タイムスタンプに対する法律の枠組みがない。独占的な契約を USPS[51]と結ぶことにより、法的拘束力のあるタイムスタンプを発行することができる。

アメリカの実績を、スイスにある UPU[52]からワールドワイドに広げることを志している。UPU は、世界の郵政事業体 180 で組織化された連合体である。UPU は、郵便物が動いた時各々の郵便機関の決済が連動する仕事をしている。UPU の提案は、物理的郵便切手をデジタル切手に変えることである。

米国では、公式な文書に個人に帰属する署名とタイムスタンプが求められる。欧州

[51] United States Postal Service：米国郵政公社
[52] Universal Postal Union：万国郵便連合

と米国の違いは、欧州の方が、法的枠組みがずっと進んでいる。欧州では法的枠組みにビジネスを合わせることがポイントである。

ドイツのビジネスプロセスに合わせるためには、「電子署名＋タイムスタンプ」で、かつ、早く、コストがかからないことである。ビジネスプロセスとは、ペーパがなくなり電子ペーパに変わることである。これは全体のビジネスプロセスで共通に言えることである。

ドイツのｅビリングでは、付加価値税の税務書類が改ざんされる脅威があるので、申請書に電子署名する。e アシーブは、長期間重要文書を保管し、改ざんされないサービスである。e スキャンは、紙をスキャンしてデジタルに変えるサービスである。テクノロジは、基礎ではなく、応用を目指している。応用アプリケーションを提供することで、官庁等のユーザーから利益を得ることを目指している。

2000 年半ばからビジネスをスタートしたが、当時ビジネスプロセスを最適化するものがなく、あったとしても不十分であった。テクノロジーを独自で開発し、サービスに統合していった。

主なユーザーは、ドイツテレコム、ドイツの携帯電話シェア 40%の携帯電話会社、経済省である。国際的企業であるレンタカーのナショナルカー、化学会社のダウケミカルもユーザーである。全てのユーザーは、テクノロジーをアプリケーションに統合して利用している。

● 質疑応答：

Q： USPS の e ポストマークは電子消印のことか。（米丸先生）

A： e ポストマークは、消印を電子化したものである。ポストスタンプしたものは、国が保証することになっている。（Jan.C.E.Wendenburg）

Q： 内容を保護し暗号化するところまで行われているのか。（米丸先生）

A： 暗号化まで行っていない。タイムスタンプのみである。（Jan.C.E.Wendenburg）

Q： ｅスキャンというサービスは、紙をスキャンしてデジタル化し、タイムスタンプを押すサービスのことか。(米丸先生)

A： スキャンしたデータに対し、デジタル署名とタイムスタンプの両方を行う。（Jan.C.E.Wendenburg）

Q： ビジネスモデルはどのような形態か。（NTT データ　遠藤）

A： タイムスタンプの提供サービス（TSA）とビジネスプロセスに組み込むためのソフトウェア（デジタル署名とタイムスタンプの両方サポート）をライセンス方式で提供する 2 通りがある。スタンダードな I／F を提供している。

当社は、ドイツでタイムスタンプに特化して認定された唯一の企業であり、タイムスタンプと署名のコンビネーションを提供できる企業としてドイツ最大の企業である。（Jan.C.E.Wendenburg）

Q： ＵＳＰＳへ採用されるためには要件を満足する必要があるが、要件が書かれたガイドラインはあるのか。（ＮＴＴデータ　櫻井）

A： ＵＳＰＳと共同で要件を作成した。機密になっているためオープンになっていない。要件を話すと時間が足らないが、主に①コンピュータセンタを提供できること、②決済ができること、③シンプルなハンドリングであること、④コンピュータセンタが安全であること、④審査や監査を受けていること、などである。パートナーであるマイクロソフトの Office バージョンに「電子署名＋タイムスタンプ」を提供しているが、USPS と共同で行った。USPS と同じものがカナダ PS にもある。そこでスタンダード化した。これを、UPU を通じて世界に広げる予定である。

日本の郵政公社に聞けば分かるかもしれないが、メールで依頼があれば、アクセス先を教える。最近スタッフの 1 人が中国、マカオ、オーストラリア、ニュージランドの郵便事業者を訪問し、テクノロジを紹介してきた。技術紹介は可能で、メンバーを紹介する。連絡を取っていただいてもよい。（Jan.C.E.Wendenburg）

Q： 文書管理プロジェクトのドメアには関わっていないのか。（米丸先生）

A： ドメア・プロジェクトは、ドイツが推進しているプロジェクトで、ドキュメントの保管方法についてスタンダード化することを目的としている。保管する時のプロセス、テクノロジーについて検討している。タイムスタンプと切り離して検討している。（Jan.C.E.Wendenburg）

Q： パートナーにドイツ PS がなかったが、ドイツ PS にはサイントラスト社があり、競合であるためか。（米丸先生）

A： その通りである。（Jan.C.E.Wendenburg）

Q：サービス料金はどのようにして決めているのか。（NTT データセキュリティ　林）

A： 1 回単位で課金する方法とプリペイド型前払い方法の 2 通りがある。料金は秘密で公開していない。多く利用して頂くユーザーは単金を安くしている。 1 ユーロより安く 10 セントより高い。数十セント／回である。（Jan.C.E.Wendenburg）

Q：サービス提供の形態は、どのようなパターンがあるのか。（NTT データ経営研　田邊）

A： プロバイダ（販売代理店）への提供と直接ユーザーへの提供の 2 通りがある。仮

想タイムスタンプソフト（VTSA）を購入すれば、プロバイダがタイムスタンプサービスを提供することができる。プロバイダへの提供の方が決済がし易い。

USPS には、電子署名とタイムスタンプの両方を提供している。AuthentiDate 社が成功した理由は、タイムスタンプのない電子署名は意味がないことが分かってきたこと、つまりタイムスタンプのない文書は改ざんの脅威があることが分かってきたことである。

USPS のポストマークには、決済とタイムスタンプの両方のサービスが含まれており、インターネットで誰もが利用できる。ライセンス方式で他の国のポスト機関、国家機関にも提供している。欧州の法律は厳しいが、これをクリアし、ハイパレベルのサービスを提供している。

欧州ではドイツ、欧州の署名法で公認されることが条件になる。公認されることにより、ユーザは裁判でも有利になる。AuthentiDate 社のタイムスタンプは、ハードとソフトのコンビネーションでクリアしている。例えば、秘密鍵は、スマートカードに保管している。これは、コモンクライテリアで認められている唯一のものである。レベル 4 をクリアしている。

HSM は現在認定されていないため使えない。現在パートナと組んで開発中で、ソフトは完成した。HSM を利用できれば、ハイパフォーマンスを実現することができる。（Jan.C.E.Wendenburg）

Q： 技術要件について確認させてほしい。秘密鍵長、ハッシュ関数、有効期限ついて説明して頂きたい。(NTT データ　櫻井）

A： 鍵長 1024 ビット、ハッシュ関数 RIPEMD-160 ビット、有効期限 3 年である。有効期限は研究当初 5 年であったが、見直した。2 年後に再チェックする予定である。ハッシュ関数 SHA-１は一般的であるが採用していない。ドイツの要求条件が世界で最もハイレベルである。（Dr.PercyDahm）

Q： ドイツで認定を受けているということは、ビジネスにプラスになっているのか。（NTT データ経営研　三谷）

A： 米国とドイツを同じタイミングで会社を設立した。会社設立のアイデアは、我々とは関係のない会社から提案された。2000 年半ばに米国から声がかかり、米国、ドイツのジョイトベンチャとして始まった。

現在ナスダックに上場し、本社はニューヨークである。 2000 年のニューエコノミーの波にのって会社を設立した。ドイツで認定を受けているのは、ブランドとしてビジネスのプラスになっている。e ビリング、e スキャンは、法的ニーズがあり、ドイツ国内で開発した。

米国のタイムスタンプをそのまま使うことはできない。欧州の要求条件はそれだ

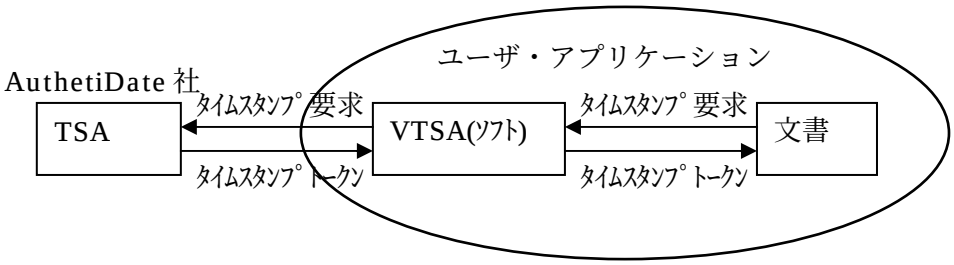
け厳しい。米国は国ではなく企業が要求条件を検討する。（Jan.C.E.Wendenburg）

Q： USPS へのライセンス方式はどのようになっているのか。（アマノ　内藤）

A： USPS の e ポストマークは、USPS が AuthetiDate 社へアウトソーシングしている。売上げは、USPS と AuthetiDate 社とで半々で分けている。（Jan.C.E.Wendenburg）

Q： ライセンス方式で提供している企業は、電子署名とタイムスタンプの両方を扱うことができるのか。（アマノ　内藤）

A： そのとおりである。タイムスタンプは AuthetiDate 社が提供しているタイムスタンプサービスを利用している。（Jan.C.E.Wendenburg）



Q： タイムスタンプ方式はどの国際標準に準拠しているのか。（アマノ　内藤）

A： RFC3161 である。（Dr.PercyDahm）

Q： なぜ認定が AuthentiDate 社１社だけなのか？（ＮＴＴデータ　遠藤）

A： 当社の商品だけが認定基準を満たしているからである。
認定されるまで時間とコストがかかる。テクニカル以外に①スタッフの無犯罪証明、②コンポーネントの内容、③スタッフの能力証明などの資料を提出した。
コンポーネントは、当然基準を満たしたものを使わなくてはならない。規制庁は、事前予告なしにいつでもオフィスに入って資料をチェックする権利がある。（Jan.C.E.Wendenburg）

Q： スケーラビリティはどれくらいか？（小関先生）

A： ハードウェアを追加することで性能向上できる。インターネットのバンド幅に性能が左右する。（Jan.C.E.Wendenburg）

Q： 今後どれくらいの利用量を見込んで設計したのか？（小関先生）

A： プロセスは、紙から電子へ移動している。真正性を証明することは重要である。電子署名だけならば利用範囲が限られる。署名した時刻を証明できるように、署名にもタイムスタンプを当然つけるべきである。
現在過度期であるが、広がり始めている。将来の市場は膨大である。TSA は、ヨーロッパと米国に１つある。現在３つ目を検討中である。（Jan.C.E.Wendenburg）

Q： 認定を受けるにあたり、企業がサービスをストップした場合の存続性はどのようになっているのか。（アマノ　内藤）

A： 企業がサービスをストップすると大きな損害が発生する。認定された企業は、保証準備金を事務局から要求される。法令では、1 つのタイムスタンプあたり、2.5 ミリオンユーロである。現在保険をかけており、保険会社を見つけるのに大変苦労した。認定されている業者と認定されていない業者との差はそこにある。認定される企業は健全な会社でなければならないので、倒産する確率は少ない。認定された企業の義務は、データを 30 年間保存しなければいけない。データに対して再署名し、非改ざん証明できる措置を講じておかなければいけない。（Jan.C.E.Wendenburg）

Q： 再署名は、AuthentiDate 社の責任で行うのか、ユーザーの責任で AuthentiDate 社が代理で行うのか。（アマノ　内藤）

A： ユーザーが行う。（Jan.C.E.Wendenburg）

Q： 原本そのものを AuthentiDate 社で保管しているのか。（アマノ　内藤）

A： 署名したものは、いつか再署名しなければならない。法律で決められている。ユーザーで保管している原本の再署名はユーザー自らしなければいけない。（Jan.C.E.Wendenburg）

Q： ３０年間ＴＳＡで保存しなければいけないデータは具体的に何か。（ＮＴＴデータ　櫻井）

A： 発行したタイムスタンプトークンそのものである。（Jan.C.E.Wendenburg）

Q： RFC3161 であれば、TSA を認証するための CA が必要であるが、ＴＳＡ用証明書を発行するＣＡの運用規定はどのようになっているか。（ＮＴＴデータ　櫻井）

A： 規制庁から発行された証明書を使っている。証明書に規制庁から発行されたことが記されているので、認定されていることが分かる。企業がサービスをストップ

する場合、規制庁がデータバンクを引き継ぐ。規制庁が 30 年間データを保管するのである。ユーザーは、その間問い合わせすることができる。（Jan.C.E.Wendenburg）

Q： 30 年保管したり保険をかけたりすることを米国でもしているのか。（ＮＴＴデータ経営研　三谷）

A： 米国ではしていない。（Jan.C.E.Wendenburg）

Q： 外国に発行したタイムスタンプもドイツが保証するのか。（米丸先生）

A： ドイツが 30 年間保証する。但し米国の USPS の場合 7 年間保存することが要求条件である。これは米国政府の要求条件ではない。（Jan.C.E.Wendenburg）

Q： ＥＵの他の状況はどのようになっているか。（大橋先生）

A： 1999 年に EU 電子署名指令が出た。各国はこれをベースに国内法として展開することになっている。そこにはタイムスタンプは書かれていない。当時電子署名のみでタイムスタンプの必要性に気付かなかった。ところが、現在になりタイムスタンプが必要であることに気付き始めている。例えば、役所の入札システム等にタイムスタンプはオプションとして要求条件に書かれるようになってきた。署名延長する場合、認定タイムスタンプは必須である。ドイツでは法律で決められている。EU 電子署名指令は最低レベルである。レベルを高くすることは各国の自由である。ドイツが最もレベルが高いが、オーストリー、イタリア、スペイン、ギリシャもレベルは高い。（Jan.C.E.Wendenburg）

Q： 時間はどのようにして作っているのか。（アマノ　内藤）

A： ドイツには時刻法があり、それに従っている。時刻は議会が決める。ＰＴＰ（物理技術連邦庁）がドイツの標準時刻を管理しており、ラジオ波を発信している。これとＧＰＳを受信して時刻比較を行っている。（Jan.C.E.Wendenburg）

Q： 時刻比較結果は定期的に監査を受けているのか。（アマノ　内藤）

A： 監視は自分たちで行っている。プロトコルに関わるデータを担当者が管理しており、その議事録を規制庁がチェックする。（Jan.C.E.Wendenburg）

Q：タイムスタンプの時刻基準を外国の時刻基準にしてほしいという要望があった場合、提供できるのか。（小関先生）

A： できない。国により時差があるので利用者が計算しなければいけない。計算した結果は正しい時刻として認められる。（Jan.C.E.Wendenburg）

Q： 時刻精度はどれくらいまで保証しているのか。（ＮＥＣ　島）

A： 1／1000 秒まで保証している。（Jan.C.E.Wendenburg）

Q： タイムスタンプのオーダーリングは保証しているのか。（ＮＥＣ　島）

A： シリアル番号がある。（Jan.C.E.Wendenburg）

Q： ｅスキャンは法的裏付けがあるのか。（日立　谷川）

A： 健康衛生法に書かれている。（Jan.C.E.Wendenburg）

Q： 紙は捨ててもよいのか。（日立　谷川）

A： 認定タイムスタンプしたものであれば、捨ててもよい。ソフトはハードに組み込まれている。タイムスタンプは、イメージ処理して保管するときに利用する。特に法律はない。署名暗号が危殆化した場合、認定されたタイムスタンプを利用しなければいけない。署名したタイミングでタイムスタンプを付与している。既にサービスを提供している。（Jan.C.E.Wendenburg）

Q： デジタルカメラの原本性を保証することと同じことか。（小関先生）

A： 法律はスキャン後に改ざんされていないことを証明するために作られた。（Jan.C.E.Wendenburg）

Q： ｅスキャンするソフト、運用の認定制度はあるのか。（日立　谷川）

A： ソフトはない。運用は疾病金庫[53]の監督庁がチェックすることになっている。（Jan.C.E.Wendenburg）

Q： 紙を捨てるタイミングはどうか。（日立　谷川）

Ａ： スキャンニング後、すぐに捨ててもよい。（Jan.C.E.Wendenburg）

Q： 領収書のスキャンニングは可能か。（日立　谷川）

A： いかなる文書もスキャンニングは可能である。大切なのは、改ざんされていないことを証明できることである。（Jan.C.E.Wendenburg）

[53] 法定社会保険組織

Q： 30 年間保存するデータの真正性を証明するために具体的にどのような措置を講じているのか。（NTT データ　櫻井）

A： 5 年に 1 回再チェックをする。その間暗号が危殆化する可能性があれば、速やかにより安全な暗号アルゴリズムで再署名する。（Jan.C.E.Wendenburg）

Q： ArchSig プロジェクト[54]に参加しているのか。（米丸先生）

A： プロジェクトが始まった時には、すでに我々のものは出来上がっていた。（Jan.C.E.Wendenburg）

Q： リサインする時、中に含めるデータは ArchSig プロジェクトで検討されたものか、それとも御社独自のものか。（米丸先生）

A： ユーザーは既に当社独自のものを使っている。（Jan.C.E.Wendenburg）

Q： 米国市場とドイツ市場とでどちらが成長するか。（NTT データ経営研　三谷）

A： 米国ではニューテクノロジを早くアダプトする必要がある。欧州はニューテクノロジに対して動きはにぶいが、やるとなれば、長く継続して、しっかりとやる。市場は米国の方が大きい。前提条件を考えた場合、欧州の方がよいが、欧州は多くの国家で成り立っており、導入に時間がかかる。UPU でイニシアティブをとったが、タイムスタンプは準役所とイニシアティブを取ることでビジネスチャンスがある。

UPU は相互認証できる機関である。UPU のスタッフは、常に世界のスタンダード技術をウォッチしている。UPU から信頼できるスタンダードができることを期待している。ドイツで署名したものが、ロシアでも検証できるようになるであろう。

昨年（2003 年）3 月、電子ポストマーク 1.0 プロジェクトがスタートした。当社は米国で実績があるので、よい状況になっている。米国で USPS，ドイツで認定を受けている。次はアジアを考えている。アジアのパートナーを探している。UPU に準拠したソフトを提供できる。ライセンス方式で提供することができる。投資が少なくて、即スタートできる。（Jan.C.E.Wendenburg）

Q： 御社の売上高と従業員数はどれくらいか？（事務局　刑部）

A： ナスダックに上場しているので、オープンにしている。売上高は 2,500 万ドル、従業員は 100 名である。（Jan.C.E.Wendenburg）

---

[54] ドイツの電子署名文書長期保存プロジェクト

Q： タイムスタンプ以外のソリューションはどのようなものがあるのか。
（NTT データセキュリティ　林）

A： ｅビリング、ｅスキャン、e アシーブなどがある。（Jan.C.E.Wendenburg）

以上

５．３　Leuven 大学（ブリュッセル、Dumortier 教授による講演）

- 訪問日程：2004 年 3 月 20 日(土)　15:00～17:00

- 場所：Leuven 大学内 Faculty Club

- 講演者：Prof. Dr. Jos Dumortier
  他の大学側参加者：Prof. Dr. Ir. Bart Preneel
  Ms. Hannelore Dekeyser

- 報告者：内藤　隆光（アマノ株式会社　e-timing ビジネス開発部理事）
  米沢　実（アマノ株式会社　総合企画室営業企画理事）

- Dumortier 教授の経歴：
  1973 年、Leuven 大学法学部卒業
  ナンシー(1974 年)、ハイデルベルグ(1975 年)にて勉学後、
  Leuven 大学研究員
  1981 年、民間国際紛争法の論文にて法学博士号取得
  1981 年～1992 年、ブリュセッルの法律事務所の弁護士としてパートタイム勤務
  1981 年～1983 年、Libre de Bruxelles　大学にて情報科学を学ぶ
  1984 年～1992 年、アントワープ大学にて情報科学の非常勤講師を務める
  1985 年～Leuven 大学にて法律と IT の非常勤講師、
  1993 年～同大学教授として勤務
  1991 年～現在に至るまで法律と ICT の分野にておいて数冊の本を出版
  ※　ベルギー連邦政府、フランドル政府、欧州委員会、及びいくつかの国立、国際的機構にて専門家として努めている。

● 講演内容：Electronic signatures and Trusted time services in Europe

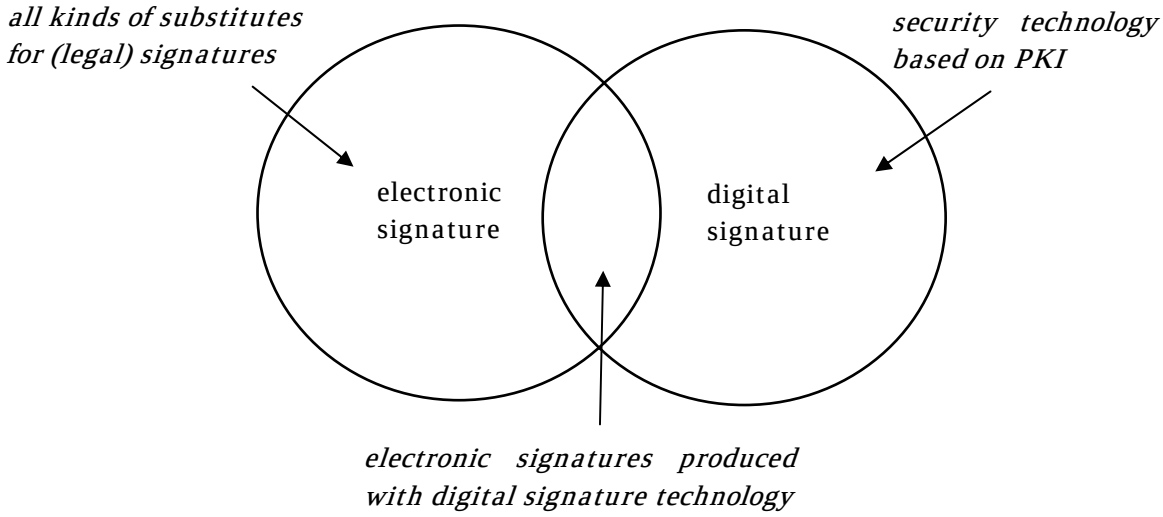
1. 欧州の電子署名法における過去の経緯

米国では 1996 年にユタ州、カリフォルニア州で電子署名法が制定、1997 年には連邦レベルで電子署名法が制定された。

この影響を受けてヨーロッパでも立法化への動きが高まりドイツ(Signaturegesetz)、イタリア(Legge Bassannin)で先導的に電子署名法を整備した。

欧州電子署名法の特徴としては以下の２つがあげられる

① “technology neutral”(技術的中立)ではなく、”digital signatures”という定義が用いられた。



【図１】

ここで【図１】により用語の定義を再確認してみると以下のようになる。

■ electronic signature (電子署名)
法的な署名の代わりになるいかなるものであり、セキュリティ的には非常広範囲なものを含んでいる。

■ digital signature (デジタル署名)
PKI に基づいたセキュリティ技術でありコンピュータデータの原本性、完全性を確保するもの。

電子署名を行なうときに digital signature 技術を活用した場合には双方を含むものとなる。ヨーロッパにおいて電子署名の立法化議論のときに法的なコンセプトの電子署名と技術的なコンセプトのデジタル署名技術が常に混同して議論されてしまった。

② 免許制の導入 ― ドイツでは任意、イタリアでは義務

1997 年のドイツ電子署名法の目的は、法的に高度なセキュリティを確保する事と企業がそれを任意に活用することが出来る事である。そして署名法に則った高度なセキュリティなものを採用した場合は、法的に高度な保証が可能となるものであった。

イタリアでは更に厳格なものであり、認証された署名のみが法的な保証を持つものとされていた。すなわち免許制の義務付けであった。

これに対しヨーロッパ市場の統一化を図っている欧州委員会(EC)は、各国独自の法規制ではなく欧州全体を包括する一つの電子署名法を作るべきだと反論し、以下の 2 つの動きにつながった。

- 欧州レベルにおける EU 指令 (European Directive 99/93/EC)の発令
  指令は各加盟国に対して提示され、各国はそれを承認した後に自国の法律の中に盛り込まなくてはならないことになっている。
- 欧州電子署名の標準化促進(EESSI: European E-Signatures Standardization Initiative) であり、これも指令として提示された。

EU 指令が与えた各国政府へのメッセージとしては、欧州市場の開放と統一化をはかるために ”KEEP YOUR HANDS OFF !!!” (手をだすな) であり、これはドイツ、イタリア政府への牽制でもあった。

指令では免許制は許容せず、認証サービスにおいて一つの欧州市場を確保する事である。認証サービスのコンセプトとは電子証明書の発行にとどまらずタイムサービス等も含まれている。

EU 指令において適格電子署名は、手書きの署名と同等と扱われている。 ここで適格電子署名とは以下の要件を満たしたものであり、法的なセキュリティを確保するために一つの統一した電子署名が必要であるとの判断からであり”Qualified”という表示が義務付けられている。加盟国の間では”Qualified Signature”は一種のパスポートと考えても差し支えない。

- 4 つのセキュリティ要求を満たした高度電子署名(Qualified Electronic Signature)であり、これは PKI をベースによるものである。
- annex 1 の要求を満たす証明書であること
- annex 2 の要求を満たした認証局により発行された証明書であること
- annex 3 の要求を満たしたハードウエアとソフトウエアを使用すること

ここで一つの注意点として、現在の適格電子署名は法的には手書署名の代用と位置

づけられており、臨時的な措置であると言える。今後電子化が進み「紙の世界」との引用関係が必要なくなった場合には、適格電子署名のコンセプトも消滅してしまう恐れがある。

欧州において、今後電子署名における手書き署名との引用関係が、徐々に減って行くと思われる。これらの観点から、適格電子署名がベストのものであるとは言えず、一つの妥協案であった。

したがって、適格電子署名と非適格電子署名の差別はするべきではないとの考え方が、EU 指令第 5 条 2 項に現れている。また、EU 指令の中には消費者保護のため各国は、電子署名制度を監督すべきであるとしている。しかしながら、この監督制度は事業者の事前承認を必要とすべきではないとしている。

また、認定制度等もあくまでも任意のものであり、各加盟国は認定を受けてない事業者がサービスを提供する事を阻んではならず、自由競争や技術革新も阻害してはならないとしている。

2. 欧州におけ現状る

All EU member states → 2003 Finland, Portugal Netherlands, Sain	All EEA countries Iceland(2001), Norway(2001) Liechtenstein(2003)
All Accession countries → exept Cyprus	All Candidate countries Bulgaria, Romania

±30 countries adopted the Directive or used it as a blueprint!

【図 2】Transposition of the Directive

EU 指令は EU 加盟国に限らず 30 カ国において電子署名の青写真として採用された。ブルガリア、ルーマニア、アイスランド、ノルウエイ等も含まれている。【図 2】

ほとんどの国においては EU 指令に準拠し認証サービス提供事業者に対しの事前承認はすべきではないとしており、所轄の監督機関への届出のみを義務付けている。

しかしながら、ドイツやオーストリアは事前承認に近い制度をとっており EU 指令とは相反している。また、監督制度の基準は、各国間で統一がされていない。　任意の認定制度を採用しているのは、まだドイツ、オーストリア、イタリア等の数カ国のみであり、認定基準も各国間で統一がはかられていないのが現状である。

各国間の Interoperability (相互運用性) に関しても大きな問題を抱えている。例えば、

アルゴリズムやパラメータは、3 カ国においてのみ記述されているに留まっている。市場に目をむけるとドイツとイタリアのみが 6 つ以上の認証サービス提供事業者があるが、他のほとんどの国は皆無か１社程度の事業者があるのみである。

適格電子証明書はまだ広範囲に使用されていない。イタリア(例：InfoCamera)とエストニア(例：EID cards)においては広範囲に発行されているが、具体的なアプリケーションとしてはほとんど使われていない。適格電子証明書の市場要求はあまりなく、e-Government(電子政府)が牽引役になっている。しかしここでも適格証明書による適格電子署名はほとんど使われていない。

e-Banking(電子銀行決済)市場で電子署名が首位に立っているが、ほとんどの国で適格電子署名が使われていない。PKI の普及が緩やかなのは、PKI が複雑であることと共通な技術的ソリューションに欠けている事が理由と思われる。

今後電子 ID カードの普及や新しい技術の導入で状況は変わるかもしれない。

3. タイムサービス及び今後の展望

タイムサービスは欧州では電子認証サービスの一つとして解釈されているので、EU 指令の基本が適用されるべきである。

すなわち

- サービス提供にあたり事前承認は不要
- 制限のない一つの開放された市場
- サービスの設立所在地のルールを適用
  （サービス提供先国のルールに左右されない）
- 手書き署名との同等性においては重要ではない（意味がない）

特に手書き署名の代用とは異なる Qualified Time Stamp は EU 指令の考え方にはうまくあてはまらないと考えられる。ここで誤解してほしくないのはネットワークサービスにおいてセキュリティは大変重要な課題であり、国家が推進役となるべきであるが、それは機能面に限定されるべきである。

今後の展望

我々はすでに EC（欧州委員会）に EU 指令の見直しに関する報告書を提出したが、ドイツ、オーストリア等の国がすでに多大な投資を行って構築した集中的な認証システムを開放するかが今後注目されるべき点である。

-

********** 講演終了**********

● 質疑応答：

原本性の証明には PKI だけで十分と思うか？という質問に対して長期保存に関しては技術的な観点で言えば再署名が必要となる。
(Dr. Preneel)

EU 指令ではタイムスタンプに関わる規制は課していないが、例えば Electronic Invoicing（電子的な請求書発行）、Electronic Procurement（電子調達）等の分野における特殊な EU 指令ではタイムスタンプの利用を義務付けている。
(Dr. Dumortier)

Legal Time(法的時刻)と考えられる時刻に関する法規があるがこれは欧州レベルではなく、各国独自のものとなっている。一日も早く欧州レベルに調和的に導入されることを期待する。
(Dr. Dumortier)

欧州におけるタイムスタンプの将来について、インターネットが普及し始めた頃には独立した Trust Service が提供されるのではないかとの見方があったが、現在においても ID カードは国から、クレジットカードは銀行からというように変化は見られていない。そのような観点から Trust Service を独立して提供するのは難しいのではないかと考える。Time Stamp Service もそれだけを独立して提供するのは難しいと思われる。例えばユーザーが求めているのは Archiving System（電子保存）と Time Stamp Service の両方の機能であったり、もっと広範囲なものを要求するのではないかと思われる。
(Dr. Preneel)

５．４　ドイツ連邦政府経済労働省（ベルリン）

● 訪問日程：2004 年 3 月 24 日（月）　10:00～12:00

● 対応者：Dr.DOMINIK GASSEN（右写真左）
Dr.TILL SCHEMMANN,LL.M.（右写真右）
Dr.Tamas Horvath（左写真、Ｄ－ＴＲＵＳＴ）

● 報告者：中嶋　勝治（セイコープレシジョン株式会社
ソリューション事業本部ソフト開発部副主査）
島　成佳　（日本電気株式会社　システム基盤ソフトウェア開発本部　主任）

● ヒアリング内容：

ドイツ連邦政府経済労働省は、ドイツ国内において電子署名を管轄している省庁である。ドイツの電子署名法の 9 条にタイムスタンプについての記述があるが、詳細な規程は特にない。タイムスタンプは、公共調達のような公的に何か時間制限のあるものに利用されていくと考えられる。現在ドイツ連邦政府経済労働省は、内務省と電子調達のプロジェクトを進めており、電子調達のシステムの中で使われる可能性がある。

ドイツの電子署名法にタイムスタンプを盛り込まれているのは、電子署名の改ざん防止と電子署名日時を特定するためと、アルゴリズムが危殆化の再に再署名のためである。ドイツ以外に電子署名法にタイムスタンプを盛り込んでいるのは韓国がある。

ドイツ国内では、サッカーくじ協会がくじの〆切時間に使えるのではないかとタイムスタンプに興味を示している。また、日本側の特許の先発明主義対策に使いたいという考えにもドイツでも検討していきたいとの回答があった。

経済労働省、内務省、いくつかの企業によって、1 年前に署名協議会が設立された。署名協議会は、市民が e ガバメントや e ビジネスの分野で活動しており、現在 31 社が参加していて今後も参加組織が増加予定である。また、電子署名カードを発行できるように助成を行っていく予定である。

電子署名カードの発行を背景には、現在証明書の発行や利用のための市民コストが高いため、市民コストを低くすることを目的としている。政府関連では、健康保険や年金関連の組織が参加している。健康保険では、医者と薬剤師にカードを発行している。

2006 年 1 月 1 日から患者用のカードを発行していく予定である。技術企画は ISIS-MTT，IETF，ヨーロッパスタンダードを使っている。アーカイブは、現在 EU で標準化が行われており，次回サンフランシスコの国際会議で標準化を働きかける予定である．

５．５　連邦公証人会（ベルリン）

● 訪問日程：2004 年 3 月 24 日（月）　14:00～16:00

● 対応者：Dr.Andreas Goerdeler　（写真左）
Stefan Altmeppen,LL.M.（写真右）

● 報告者：中嶋　勝治（セイコープレシジョン株式会社
ソリューション事業本部ソフト開発部　副主査）
島　成佳（日本電気株式会社　システム基盤ソフトウェア開発本部　主任）

● ヒアリング内容：

公証人は、ドイツにおいて独立した法律家で国から認定を受けており、国の一部でもある。連邦公証人会では、2002 年に官庁でオンラインのデータ交換可能な制度の整備を行っており、2004 年からは e-mail でのデータ交換も可能となる。EU 全体では，2007 年までに商業登記を電子的な手続きが可能となるように EU 勧告ができており、現在整備中である。

連邦公証人会の CA は、ドイツ国内で 3 番目に認定された。認定には費用が 2 万 5 千ユーロ必要であった。今後 3 年おきの定期審査には１万ユーロ必要となる。CA は秘密鍵の鍵長が 1024 ビットで、署名、暗号、認証のための証明書を発行している。証明書や証明書廃棄リストを LDAP サーバに管理/格納している。また、証明書有効性確認サービス(OCSP)やタイムスタンプサービスも行っている。

公証人連合会では、1999 年から電子署名のインフラと公証人ネットワーク構築を行っている。公証人は公証人ネットワークへの接続に ID カードを使用する予定である。

また、公証人ネットワークは利用促進のため裁判所にも導入する予定である。

ドイツでの電子署名の取り組みは、e ガバメントを通して 2002 年，2003 年と進めている。市民が官庁との手続きにおいて証明書を使うことを目的としている。

しかし、市民は州政府における手続きは多いが官庁との間の手続きが少ないことが問題となっているが、州政府が進める事例として開始することを目的としている。また、ドイツ国内では、社会保険との関連で市民に JOB カードを発行予定である。JOB カードは、4 万枚程度発行予定であり、ドイツ連邦政府経済労働省の研究チームにおいて、電子署名の普及において新しいビジネスモデルの検討を行っている。

日本の電子公証には、確定日付を付与する業務があり、公証人が文書に日付けを付与して署名する。ドイツでも同様の業務が可能かもしれないと回答をうけた。

このときタイムスタンプの必要性が特になるなるとのことである。ただし、確定日付サービスは、紙の文書の場合 20 から 30 ユーロであるが電子文書のサービスは行っていないとのことである。

公証人連合会では、タイムスタンプの必要性を次のように述べた。裁判では、裁判所に文書が提出されるまでの手順が重要である。公証人の時刻付与は、証拠性として高いが公証人が署名した時間から文書が有効となる。文書を作成した時点での時刻を保証したい場合はタイムスタンプが必要となる。

おわりに

本年度の調査研究分科会では、タイムスタンプに関連する海外動向を把握するために、ドイツおよびベルギーへの訪問調査を実施した。

基本的な問題意識は、タイムスタンプが法律上明記されている国において、その立法経緯、具体的な関連市場動向に関する情報を収集することであり、行政機関・民間企業・大学に対してディスカッションを実施した。参加者の意識も高くディスカッション内容は、技術面・法制度面・対象マーケット等と幅広いものになった。

やはり印象に残っているのは、ドイツ電子署名法の緻密さとその考え方である。民間サービスに対し高いレベルの技術的・運用的ハードルを越えることを要求する一方、それをクリアしたサービスを利用している国民に対しては、万一サービスが停止しても行政側が全面的にバックアップを行うというスキームにはかなり説得力があった。

タイムスタンプの法制度化を行うことのみで、それを活用した電子政府・電子商取引の活性化が実現するわけではないだろうが、その「必要条件」になる可能性は十分あるのではないだろうか。

また、どの訪問先の方々も、日本でタイムスタンプが注目されつつあること自体にかなり興味をもたれていたことも印象深い。行政機関の方から、今後も是非タイムスタンプについて両国で是非交流を深めたいというありがたいコメントもいただいたことも付け加えておく。

最後に、今回の調査企画において全面的にご協力いただき、副団長として参加していただいた神戸大学の米丸先生と、全工程において調査団活動の側面支援をしていただいたフォーラムジャパンの尾内氏に改めて感謝の念を表したい。

今回の調査成果が今後のタイムビジネス普及・啓発の一助になれば幸いである。

タイムビジネス推進協議会
企画部会・調査研究分科会主査
ＮＴＴデータ経営研究所
三谷 慶一郎

【関連資料】

● デジタル署名法

情報サービスおよび通信サービスの大綱条件の規制のための法律〔97 年 7 月 22 日公布〕米丸恒治訳[55]

(Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste；Informations- und Kommunikationsdienste-Gesetz；IuKDG, v. 22. 7. 1997, BGBl. I S. 1870)

本法は、以下の条文からなるオムニバス法である。特に、本稿の観点からは、第１条から第３条までの新法の制定が重要であると考えられるので、日本語訳を掲げる。その他の部分については、割愛したい。

第１条　テレサービスの利用に関する法律(Gesetz über die Nutzung von Teledinesten；Teledienstegesetz；TDG)

第２条　テレサービスにおけるデータ保護に関する法律(Gesetz über den Datenschutz bei Teledinsten；Teledienstedatenschutzgesetz；TDDSG)

第３条　デジタル署名法(Gesetz zur digitalen Signatur；Signaturgesetz；SigG)

第４条　刑法典改正

第５条　秩序違反法改正

第６条　青少年に害悪を及ぼす文書の頒布に関する法律の改正

第７条　著作権法改正

第８条　価格表示法改正

第９条　価格表示令改正

第１０条　統一命令秩序への復帰

第１１条　施行

なお、本法は、7 月 22 日に公布され、７条(98 年 1 月 1 日施行)を除くその他の条項は、8 月 1 日からすでに施行されている。

以下の資料は、情報・通信サービス大綱法のうち、新たに法律として制定されることとなった第３条のデジタル署名法の試訳である。

第３条　デジタル署名法(Gesetz zur digitalen Signatur；Signaturgesetz；SigG)

「

〔目的と適用範囲〕

第１条　本法の目的は、デジタル署名が安全なものとして通用しかつ署名の偽造または署名されたデータの改ざんを信頼性をもって確認することのできる、デジタ

[55] デジタル署名法の和訳は、「米丸恒治「ドイツ流サイバースペース規制－情報・通信サービス大綱法の検討」 立命館法学 255 号 141-194 頁に所収のものを収録した。」

ル署名のための大綱条件を創出することである。

(2)　本法によるデジタル署名の利用が法令により定められていない限りで、デジタル署名のための別の手続の利用をすることは、自由である。

〔定義〕

第２条　本法におけるデジタル署名は、私的署名キー(privater Signaturschlüssel)によって生成されたデジタルデータに対する印(Siegel)であり、認証機関(Zertifizierungsstelle)または第３条による行政庁の署名キー証明証(Signaturschlüssel-Zertifikat)が備えられたそれに対応する公的キーを用いることにより、署名キーの所有者およびデータが改ざんされていないことを認識させるものをいう。

(2)　本法における認証機関は、公的署名キーがある自然人のものであることを証明し、かつそのための本法第４条による免許を有する自然人または法人をいう。

(3)　本法における証明証(Zertifikat)とは、公的署名キーがある自然人のものであることについての、デジタル署名を付されたデジタル証明(以下、署名キー証明証という。)、または署名キー証明証に一義的に関連しながらさらに別の記述を含む別のデジタル証明(以下、属性証明証(Attribut-Zertrifikat)という。)をいう。

(4)　本法におけるタイムスタンプとは、特定のデジタルデータが特定の日時に認証機関に提出されたことについての、デジタル署名を付された認証機関のデジタル証明をいう。

〔所管行政庁〕

第３条　　免許の付与および証明証の署名に用いられる証明証の発行、ならびに本法および第１６条の法規命令の遵守の監視は、電気通信法第６６条による行政庁の権限とする。

〔認証機関の免許〕

第４条　　認証機関の活動は、所管行政庁の免許を必要とする。免許は、申請に基づき与えるものとする。

(2)　申請者が認証機関の活動に必要な信頼性を有しないことをうかがわせる事情があるとき、申請者が認証機関の活動に必要な専門知識を有することを証明しないとき、または活動の開始に際して本法および第１６条による法規命令による認証機関の活動に必要なその他の要件がないと予想されるときは、免許はこれを与えないものとする。

(3)　認証機関の所有者として活動の基準となる法令を遵守する保障のある者は、必要な信頼性を有する。認証機関の活動に携わる者がそれに必要な知識、経験および技能があるときは、必要な専門知識がある。本法および第１６条の法規命令のセキュリティ要件を満たす措置を所管行政庁に適時にセキュリティ計画と

して示し、かつ所管行政庁により承認された機関によりその実施が検査され かつ証明されたときは、認証機関の活動のためのその他の要件が満たされる。

(4)　認証機関が活動の開始に際しおよび活動中に本法および第１６条による法規命令の要件を満たすことを確保するために必要である限りで、免許に付款を付することができる。

(5)　所管行政庁は、証明証の署名のために用いられる署名キーについて証明証を発行する。認証機関による証明証の付与のための規定は、所管行政庁にこれを準用する。所管行政庁は、その発行した証明証を公衆の到達し得る電気通信網を通じて何人にも常に審査可能かつ呼び出し可能であるようにしておかなければならない。認証機関の住所および電話番号、その発行した証明証の効力停止、認証機関の活動の中止および禁止ならびに認証機関の免許の取消または撤回についての情報についても同様とする。

(6)　本法および第１６条による法規命令による公的給付については、その費用(手数料および立替金)を徴収する。

〔証明証の付与〕

第５条　認証機関は、証明証を申請する者の本人確認を確実に行わなければならない。認証機関は、公的署名キーが本人確認された者のものであることを署名キー証明証により確認し、かつこの署名キー証明証および属性証明証を公衆の到達し得る電気通信網を通じて何人にも常に審査可能でありかつ署名キー所有者の同意を得て呼び出し可能であるようにしておかなければならない。

(2)　認証機関は、その認証機関に対し第三者の代表権の取り入れのためのその第三者の承認または許可が確実に証明される限りで、申請者の求めにより、申請者にその第三者の代表権があることならびに職業法上の許可またはその他の許可についての表示を署名キー証明証または属性証明証に取り入れなければならない。

(3)　認証機関は、申請者の求めにより、その氏名にかえて仮名を証明証に取り込まなければならない。

(4)　認証機関は、証明証のためのデータが気づかれずして偽造または改ざんされることのできないような措置を講じなければならない。認証機関は、さらに、私的署名キーの秘密保持が保障されるための措置も講じなければならない。私的署名キーの認証機関での保存は許されない。

(5)　認証機関は、認証活動の遂行のために信頼のおける者をおかなければならない。署名キーの準備および署名の生成のために、認証機関は、第１４条による技術的な装置をおかなければならない。第１項第２段による証明証の審査を可能とする技術的な装置についても同様とする。

〔教示義務〕

第６条　認証機関は、第５条第１項による申請者に対し、信頼性のあるデジタル署名およびその確実な検査に資するために必要な措置につき教示しなければならない。認証機関は、申請者に対し、第１４条第１項および第２項の要件をどの技術的な装置が満たすものであるか、ならびに私的署名キーにより生成されたデジタル署名の帰属について、教示しなければならない。認証機関は、申請者に対して、デジタル署名を付されたデータについて、すでに存する署名のセキュリティ度が時間の経過により低下する前に、必要があれば新たに署名をしなおさなければならないことを指示しなければならない。

〔証明証の内容〕

第７条　署名キー証明証は、次の各号に掲げる事項を含んでいなければならない。

１　混同する可能性がある場合は付加語を付した、署名キー保有者の名称、または署名キー保有者のものである、かかるものとして識別されなければならない混同不可能な仮名

２　帰属する公的署名キー

３　署名キー保有者の公的キーおよび認証機関の公的キーに用いることのできるアルゴリズムの表示

４　証明証の通し番号

５　証明証の有効期間の始期と終期

６　認証機関の名称

７　署名キーの利用が種類および範囲につき特定の用途に制限されているものであるかどうかの表示

(2)　第三者のための代表権の表示ならびに職業法上またはその他の許可についての表示は、これを署名キー証明証および属性証明証に取り入れることができる。

(3)　署名キー証明証には、関係者の承認があるときにのみ、その他の表示を取り入れることができる。

〔証明証の効力停止〕

第８条　認証機関は、署名キー保有者またはその代理人が要求したとき、第７条についての虚偽表示に基づき証明証を取得したものであるとき、認証機関がその活動を終了したときでなおかつその活動が他の認証機関により継続されないとき、または所管行政庁が第１３条第５項第２段により効力停止を命じたときは、証明証を効力停止にしなければならない。効力停止は、その効力が生じる日時を含まなければならない。過去にさかのぼっての効力停止は、許されない。

(2)　証明証が第三者の表示を含むものであるときは、この第三者もこの証明証の効力停止を求めることができる。

(3)　所管行政庁は、認証機関がその活動を停止するとき、またはその免許が取り消されまたは撤回されるときは、それが第４条第５項により発行した証明証を効力停止にする。

〔タイムスタンプ〕

第９条　認証機関は、求めがあったときは、デジタルデータにタイムスタンプを付さなければならない。第５条第５項第１段および第２段は、これに準用する。

〔記録〕

第１０条　認証機関は、本法および第１６条による法規命令の遵守のためのセキュリティ措置ならびに発行した証明証について、データおよびそれが改ざんされていないことを常に審査し得るように、記録しておかなければならない。

〔活動の中止〕

第１１条　認証機関は、その活動を中止するときは、できるだけすみやかに所管行政庁にその旨を報告し、その活動を中止した際に効力を有している証明証を他の認証機関に引き継ぐよう手配するか、またはその証明証の効力を停止しなければならない。

(2)　認証機関は、第１０条による記録を、証明証を引き継いだ認証機関またはその他の場合には所管行政庁に引き渡さなければならない。

(3)　認証機関は、破産または和議手続の開始の申請は、所管行政庁に遅滞なく届け出なければならない。

〔データ保護〕

第１２条　認証機関は、個人関連データは、関係者自身において直接的にのみ、および証明証の目的のためにそれが必要である限りにおいてのみ収集することができる。第三者のデータ収集は、関係者の承認がある場合にのみ許される。第１段にあげる目的以外の目的のためには、データは、この法律またはその他の法令が許容しまたは関係者がそれを承認したときにのみ利用することができる。

(2)　仮名を用いている署名キー保有者にあっては、認証機関は、犯罪行為もしくは秩序違反行為の訴追のため、公共の安全と秩序に対する危険を防止するため、または連邦および州の憲法保護庁、連邦諜報局、国防軍防諜局もしくは関税取締局の法律上の事務遂行に必要な限りでのみ、その本人確認についてのデータを求めに応じて権限ある機関に引き渡すことができる。報告は、記録にとどめなければならない。情報を求める行政庁は、署名キー保有者に対し、法律上の事務の遂行がもはや侵害されなくなったとき、または署名キー保有者の教示することに対する利益が重大であるときは、ただちに仮名の暴露について教示しなければならない。

(3)　連邦データ保護法第３８条は、データ保護規定違反の根拠がない場合にお

いても検査をすることができるという基準で、これを適用する。

〔義務の統制と執行〕

第１３条　所管行政庁は、認証機関に対し、本法および法規命令の遵守を確保するための処分をすることができる。所管行政庁は、そのため特に、適当でない技術的な装置の利用を禁止し、認証機関の活動を暫定的に全部または一部中止させることができる。第４条による免許を持てないにもかかわらず免許を得ていると思われる者については、認証の活動の中止を命ずることができる。

(2)　第１項第１段の監視の目的のために、認証機関は所管行政庁が通常の営業時間中に事務所または事業所に立ち入ることを認め、求めに応じて該当する書籍、帳簿、文書、書類、およびその他の記録を閲覧に供し、報告を行い、および必要な補助を行わなければならない。報告義務者は、その回答が自らまたは民事訴訟法第３８３条第１項第１号ないし第３号に掲げられている者を、犯罪行為の訴追もしくは秩序違反取締法による手続の危険にさらすような質問への回答を拒むことができる。報告義務者は、この権利について、告げられるものとする。

(3)　本法もしくは法規命令の義務を履行しない場合、または免許の拒否理由の一つが生じた場合は、所管行政庁は、第１項第２段の処分によっては目的が達せられないときは免許を撤回しなければならない。

(4)　免許の取消もしくは撤回の場合、または認証機関の活動の中止の場合は、所管行政庁は別の認証機関によるその活動の引き受けまたは署名キー保有者との契約の精算を確保しなければならない。免許された活動が継続されない場合は、破産または和議手続の開始の申請に際しても同様とする。

(5)　認証機関により発行された証明証の効力は、免許の取消または撤回によっても影響を受けない。所管行政庁は、証明証が偽造されもしくは十分に偽造から保護されていないこと、または署名キーの利用にさいして用いられている技術的装置が、デジタル署名の気づかれない偽造もしくは署名されたデータの気づかれない改ざんを許すようなセキュリティ上の欠陥を持つことを示す事情があるときは、証明証の使用中止を命令することができる。

〔技術的装置〕

第１４条　署名キーの生成および保存ならびにデジタル署名の生成および検査のためには、デジタル署名の偽造および署名されたデータの改ざんを確実に認識可能にしかつ私的署名キーの不正な利用から保護する、セキュリティ措置を施された技術的装置を必要とする。

(2)　署名されるべきデータの表示のためには、デジタル署名の生成をあらかじめ一義的に示しかつどのデータにデジタル署名が関連しているかを確認させるセキュリティ措置を施された技術的装置を必要とする。署名されたデータ

の審査のためには、署名されたデータが変更されていないかどうか、どのデータにデジタル署名が関連しているか、およびどの署名キー保有者にデジタル署名が属するかを確認させるセキュリティ措置を施された技術的装置を必要とする。

(3)　署名キー証明証を第５条第１項第２段により審査しうることのできるまたは呼び出すことのできる技術的装置にあっては、証明証目録を不正な変更および不正な呼び出しから保護するための措置を必要とする。

(4)　第１項ないし第３項による技術的装置にあっては、技術の水準に照らし十分に審査されていること、および所管行政庁により承認された機関により必要条件をみたしていることを確認されていることを必要とする。

(5)　ヨーロッパ連合の他の構成国においてまたはヨーロッパ経済地域についての協定のその他の締約国において通用している規制もしくは要件にしたがい適法に製造されもしくは流通しており、かつ同等のセキュリティを保障された技術的装置にあっては、第１項ないし第３項によるセキュリティ技術上の仕様にかかわる要件は満たされているとみなす。説明資料を付された個別事例においては、所管行政庁の求めに応じて、第１段の要件が満たされていることが証明されなければならない。第１項ないし第３項にいうセキュリティ技術上の仕様に関する要件の証明のために所管行政庁により承認された機関の確認証の提示が定められている場合において、ヨーロッパ連合の他の構成国またはヨーロッパ経済地域についての協定のその他の締約国において許可された機関による確認証についても、その機関の審査報告書の基礎とされている技術的要件、審査および検査手続が所管行政庁により承認された機関のそれと同等のときは、それを考慮する。

〔外国の証明証〕

第１５条　ヨーロッパ連合の他の構成国またはヨーロッパ経済地域についての協定のその他の締約国でなされた外国の証明証が付されている公的署名キーを付されて審査されることのできるデジタル署名は、それが同等のセキュリティをもっているとみられる限りにおいて、本法によるデジタル署名と同等とみなす。

(2)　第１項は、相当の超国家的または国家間の約定がなされている限りにおけるその他の国についてもこれを準用する。

〔法規命令〕

第１６条　連邦政府は、次の各号について、法規命令により第３条ないし第１５条の実施のために必要な法令を制定する権限を有する。

１　認証機関の免許の付与、取消および撤回の手続ならびに認証機関の活動の停止の際の手続の細目

2　第４条第６項による手数料支払い義務の要件および手数料の額
3　認証機関の義務の細目
4　署名キー証明証の有効期間
5　認証機関の統制の細目
6　技術的装置ならびに技術的装置の審査および要件が満たされていることの確認についての細目的要件
7　新たなデジタル署名が与えられるときの期間および手続

」

電子署名に関する命令(署名令)（旧署名令）　1997 年 10 月 22 日　　〔抄訳〕
(Verordnung zur digitalen Signatur (Signaturverordnung - SigV) v. 22. Okt. 1997 (BGBl. I S. 1870, 1872))

米丸恒治訳

Inhaltsübersicht

§ 1 Verfahren bei Erteilung, Rücknahme und Widerruf von Genehmigungen
(第１条　免許の付与、取消および撤回の手続)

(2) Zur Prüfung der Voraussetzungen für die Erteilung der Genehmigung trifft die zuständige Behörde die erforderlichen Feststellungen. Sie kann vom Antragsteller verlangen, daß dieser erforderliche Unterlagen, insbesondere einen aktuellen Handelsregisterauszug und aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für die gesetzlichen Vertreter der Zertifizierungsstelle, beibringt. Zur Feststellung der erforderlichen Fachkunde hat der Antragsteller darzulegen, daß das am Zertifizierungsverfahren oder an der Ausstellung von

Zeitstempeln beteiligte Personal über die erforderlichen beruflichen Qualifikationen verfügt. (必要な専門知識の確認のためには、申請者は、認証手続またはタイムスタンプの生成に関わる職員が必要な職業上の能力を有していることを説明しなければならない。)

§ 4 Unterrichtung des Antragstellers (第４条　申請者の教示)

(1) Die Zertifizierungsstelle hat einen Antragsteller im Rahmen des § 6 Satz 1 und 3 des Signaturgesetzes insbesondere über folgende erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der digitalen Signatur zu unterrichten:

((1)　認証機関は、申請者に対し、署名法６条第１段および第３段の枠内で、デジタル署名のセキュリティの確保のために、特に、以下の必要な措置を教示しなければならない。)

5. Soweit für die Verwendung signierter Daten ein Zeitpunkt von erheblicher Bedeutung sein kann, ist ein Zeitstempel anzubringen.(５　署名されたデータの利用に関して日時が重要な意味を有することがあるかぎりで、タイムスタンプを付すものとすること)

6. Werden Daten über längere Zeit in signierter Form benötigt, ist gemäß § 18 erneut eine digitale Signatur anzubringen.(６　データが、比較的長期にわたり署名された形式で必要とされるときは、第 18 条にしたがい、新たにデジタル署名を付すものとすること)

§ 10 Zuverlässigkeit des Personals (第１０条　職員の信頼性)

Die Zertifizierungsstelle hat sich von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren oder an der Ausstellung von Zeitstempeln mitwirken, zu überzeugen. Sie kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren und der Ausstellung von Zeitstempeln auszuschließen.

(認証機関は、認証手続またはタイムスタンプの生成に関与する職員の信頼性について、確信のもてる状況でなければならない。……（中略）……信頼性のない職員は、認証手続およびタイムスタンプの生成から排除するものとする。)

§ 11 Schutz der technischen Komponenten (第１１条　技術的コンポーネントの保護)

Die Zertifizierungsstelle hat Vorkehrungen zu treffen, um private Signaturschlüssel und die zum Erstellen der Zertifikate und Zeitstempel sowie zum Nachprüfbarhalten der Zertifikate eingesetzten technischen Komponenten vor unbefugtem Zugriff zu schützen.(認証機関は、私的署名キーならびに証明書およびタイムスタンプの生成や証明書の検証のために用いられる技術的な装置に権限を有しない者がアクセスすることから保護するための措置をなさなければならない。)

§ 16 Anforderungen an die technischen Komponenten (第１６条　技術的コンポーネントの要求事項)

(5) Die technischen Komponenten, mit denen Zeitstempel nach § 9 des Signaturgesetzes erzeugt werden, müssen so beschaffen sein, daß die zum Zeitpunkt der Erzeugung des Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Betreiber erkennbar werden.(署名法第９条によるタイムスタンプを生成する技術的コンポーネントは、タイムスタンプの生成の日時に妥当する法律上の時を、改竄されることなくタイムスタンプに取り込む仕様を有していなければならない。この技術的コンポーネントのセキュリティ技術上の変更は、運転者に認識可能なものでなければならない。)

§ 18 Erneute digitale Signatur (第１８条　再(新たな)デジタル署名)

Werden Daten über längere Zeit in signierter Form benötigt, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 als geeignet beurteilt sind, so sind die Daten vor Ablauf des Zeitpunktes der Eignung der Algorithmen und zugehörigen Parameter mit einer neuen digitalen Signatur zu versehen. Diese muß mit neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere digitale Signaturen einschließen und einen Zeitstempel tragen.

(データが、その作成および検査のために利用されたアルゴリズムおよび付属のパラメータが第１７条２項により適切であると判断される期間よりも長期間にわたって署名された形式で保たれる必要があるときは、そのデータには、アルゴリズムおよび付属のパラメータの適性が失われる前に、新たなデジタル署名を付さなければならない。新デジタル署名は、新たなアルゴリズムまたは付属のパラメータでなさなければならず、以前のデジタル署名を含みかつタイムスタンプを有していなければならない。)

● EU 電子署名指令

米丸恒治(訳)[56]

電子署名のための共同体の枠組に関する 1999 年 12 月 13 日の欧州議会および欧州連合理事会の指令 1999／93／EC
(Directive 1999/93/EC of The European Parliament and of The Council of 13 December 1999 on a Community framework for electronic signatures, O.J. L 13/12 (19. 1. 2000)).

欧州議会および欧州連合理事会は、
欧州共同体設立条約、および特に第４７条第２項、第５５条および第９５条を考慮し、
委員会からの提案(1)を考慮し、
経済社会委員会の見解(2)を考慮し、
地域委員会の見解(3)を考慮し、
条約第２５１条に定める手続にのっとり(4)、

(1) OJ C 325, 23. 10. 1998, p. 5.
(2) OJ C 40, 15. 2. 1999, p. 29.
(3) OJ C 93, 6. 4. 1999, p. 33.
(4) Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243, 27. 8. 1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal). Council Decision of 30 November 1999.

以下の諸点を考慮したがゆえに、

(1) 1997 年 4 月 16 日に、委員会が、欧州議会、理事会、経済社会委員会および地域委員会に対し、電子商取引における欧州のイニシャチブについての連絡文書を提出したこと、

(2) 1997 年 10 月 8 日に、委員会が、欧州議会、理事会、経済社会委員会および地域委員会に対し、電子通信におけるセキュリティおよび信頼性確保についての連絡文書ーデジタル署名および暗号のための欧州枠組に向けてーを提出したこと、

(3) 1997 年 12 月 1 日に、理事会が、委員会に、欧州議会および理事会のデジタル署名についての指令案を可及的速やかに提案することを要請したこと、

(4) 電子通信および電子商取引が、「電子署名」およびデータの真正確認(Authentication)を許容する関連サービスを必要としていること、構成国における電子署名の法的承認および認証サービスプロバイダの認定(Accreditation)に関する異なった規定が、電子通信および電子商取引の利用にとっての明白な障害を生み出すかもしれないこと、他方、電子署名に適用される条件に関する明確な共同体枠組が新技術への確信およびそれの

[56] ＥＵ電子署名指令の訳文は、米丸恒治訳「〔資料〕ＥＵ電子署名指令」立命館法学 268 号 276-292 頁(2000 年)のものを利用した。なお、同書では、「仮名」とすべき部分を「匿名」と訳していた部分を、本資料では「仮名」と修正している。

一般的な受容を強めるであろうこと、構成国における立法が内部市場における財およびサービスの自由な移動を妨げてはならないこと、

(5) 電子署名製品の互換性(interoperability)が促進されるべきであること、条約第１４条にしたがい内部市場は財の自由移動が確保される内部境界なき区域から成り立つこと、二重利用製品の輸出統制のための共同体体制を構築する 1994 年 12 月 19 日の理事会規則 EC3381／94(5) および二重利用製品の輸出統制に関して理事会により採択された共同行動についての 1994 年 12 月 19 日の理事会決定 94／942／CFSP(6) に関わらず、内部市場内での自由移動を確保しかつ電子署名に対する信頼をえるために電子署名製品に対する必須要求事項がみたされなければならないこと、

(5) OJ L 367, 31. 12. 1994, p. 1. Regulation as amended by Regulation (EC) No 837／95 (OJ L 90, 21.4.1995, p. 1).

(6) OJ L 367, 31. 12. 1994, p. 8. Decision as last amended by Decision 99／193／CFSP (OJ L 73, 19. 3. 1999, p. 1).

(6) 本指令が公共の秩序または公共の安全にかかわる国内規定が適用される範囲の情報の秘密に関するサービスの提供を整合化するものでないこと、

(7) 内部市場が人の自由移動を確保し、その結果欧州連合の市民および住民はその住所を有する国以外の国の行政庁により取り扱われる必要のある機会がますます増加しているがゆえ、電子通信の有用性はこの点について大きな役割を果たし得るであろうこと、

(8) 急速な技術発展およびインターネットのグローバルな性格が、データの電子的な真正確認を可能とするさまざまな技術およびサービスに対して開かれたアプローチを必要としていること、

(9) 電子署名が極めてさまざまな環境および応用の中で、したがって電子署名に関するかまたはそれを用いるさまざまな新サービスおよび製品の中で用いられるであろうこと、かかる製品およびサービスの定義が証明証の発行および管理に限定されるべきものではなく、電子署名を用いたまたはそれに補助的なその他のサービスおよび製品、電子署名に関わる登録サービス、タイムスタンプサービス、ディレクトリサービス、コンピューティングサービスまたは相談サービスをも含むべきであること、

(10) 内部市場が、認証サービスプロバイダの競争力を向上させるために、そして国境にかかわらず安全な方法で電子的に情報および取引を交換する新たな機会を消費者およびビジネスに提供するために、認証サービスプロバイダに国境を越えた活動を展開することを可能ならしめること、オープンネットワークを通じて認証サービスの共同体全域での提供を刺激するために、認証サービスプロバイダは、事前の許認可なくそのサービスを提供する自由を有すべきものであること、事前の許認可とは、当該認証サービスプロバイダがその認証サービスを提供するまえに国内行政庁から得なければならないあらゆる許可のみならず、同一の効果を有するその他の措置をも含まねばならないこと、

(11) サービス提供の水準強化を目指す任意認定制度が、進展する市場が求めるレベルの信頼性、セキュリティおよび質に向けたプロバイダのサービスのさらなる発展のため

の適切な枠組を認証サービスプロバイダに提供すると思われること、かかる制度が、認証サービスプロバイダ間における最善の実践の発展を促進すべきであること、認証サービスプロバイダが、かかる認証制度への参加およびそれからの便益の享受については自由に任されているべきであること、

(12) 認証サービスが、公共団体または法人もしくは自然人が国内法に適合して設立されているときには、それらのいずれによっても提供されることができること、構成国が任意認定制度の範囲外で活動することを認証サービスプロバイダに禁止すべきでないこと、かかる認定制度が認証サービスについての競争を低減しないよう確保すべきであること、

(13) 加盟国が、本指令において定められた規定の遵守の監視をどのように確保するかは決めてもよいこと、本指令が、民間部門に基礎をおく監視システムの構築を阻むものではないこと、本指令が適用可能なあらゆる認定制度のもとで監視されるよう申請することを認証サービスプロバイダに義務づけるものではないこと、

(14) 消費者ニーズとビジネス・ニーズとのバランスをとることが重要であること、

(15) 付属書IIIが、先進電子署名の機能を確保するための安全署名作成装置の要求事項を定めていること、それが、かかる装置が作動する完全なシステム環境をカバーするものではないこと、内部市場が機能するために、委員会および加盟国に、安全署名装置の付属書IIIとの適合性評価を委ねられた機関の指定を可能にするよう迅速な行動を求めていること、市場ニーズに適合するためには適合性評価は適時かつ能率的でなければならないこと、

(16) 本指令が、共同体内部で電子署名の利用および法的承認に貢献すること、規制枠組が、特定数の参加者間の私法上の任意の合意に基づく閉鎖的なシステムの内部でのみもっぱら利用される電子署名については必要ないこと、電子的に署名されたデータを受け取ることについて当事者間で方式および条件について合意する自由が、国内法により認められた範囲で尊重されるべきであること、かかるシステムにおいて利用される電子署名の法的効力および争訟手続における証拠手段としての許容性を認めるべきであること、

(17) 本指令が、国内の契約法、特に契約の締結および履行に関するそれ、または署名に関するその他の契約外の形式規定を整合化することを目標としてはいないこと、それゆえ、電子署名の法的効力についての規定は、契約の締結または契約締結の場所の確定に関する構成国の形式規定に関わらないものであること、

(18) 署名作成データの保存および複写は、電子署名の法的有効性を危殆化せしめる得ること、

(19) 電子署名が、公共部門においては、国家行政および共同体行政の内部で、ならびにこれら行政間、およびこれらと市民および経済参加者の間での通信において導入されること、それはたとえば公共調達、租税、社会保障、保健および司法の分野において

用いられるであろうこと、

(20) 電子署名の法的効果に関する整合化された基準によって、共同体全域に統一性のある法的枠組が樹立されるであろうこと、構成国の国内法においては、手書き署名の法的有効性に関する多様な要件が定められていること、証明証は、電子的に署名する人物の同一性を確認するために用いられることができること、適格証明証に基づく先進電子署名は、より高度なセキュリティ水準を目ざしていること、適格証明証に基づきかつ安全署名作成装置により作成される先進電子署名は、手書き署名に関する要件が充足されるときにのみ法的に手書き署名と同等とみなされることができること、

(21) 電子的真正確認方法の一般的な受容を促進するために、電子署名がすべての構成国において裁判手続きにおいて証拠手段として利用されることができることが確保されねばならないこと、電子署名の法的な承認は、客観的な基準に基づくべきであり、当該認証サービスプロバイダの許認可と結び付けるべきではないこと、電子文書および電子署名を利用することができる法分野の確定は、構成国法に服すること、本指令は、本指令の要件との適合について決定する構成国の裁判所の権限には関わらないのであり、それは、証拠手段の裁判所による自由な評価に関する構成国の規定にも関わらないこと、

(22) 認証サービスを公に提供する認証サービスプロバイダは、責任に関する構成国の規定に服すること、

(23) 国際的な電子商取引の発展は、第三国の関与の下での国境を越えた合意を必要としていること、世界的な互換性を確保するために、認証サービスの相互承認に関する、第三国との多数国間規則に関する合意が有益でありえようこと、

(24) ユーザの電子通信および電子商取引への信頼を強化するために、認証サービスプロバイダは、データ保護立法および個人のプライバシーを遵守しなければならないこと、

(25) 証明証における仮名の利用についての規定は、構成国が共同体法または国内法により人物の同一性確認を求めることを妨げるべきではないこと、

(26) 本指令の実施のために必要な措置は、委員会に付与された執行権限の行使のための手続を定める 1999 年 6 月 28 日の理事会決議(1999／468／EC(1))によりとられるものとすること、

(1) OJ L 184, 17. 7. 1999, p. 23.

(27) 委員会は、本指令の施行後 2 年において、とりわけ技術進歩または法的環境の変化が本指令の宣言された目標の実現にとって障害をもたらさないことを確保するために点検を実施すること、委員会は、関連技術分野の影響を審査し、欧州議会および理事会にこの点に関し報告書を提出するものとすること、

(28) 条約第５条に定められた補完性および比例性の原則により、電子署名および関連サービスの提供に関する整合化された法的枠組の創出の目標は、構成国によっては十分には達成されることはできず、かつそれゆえ共同体によりよりよく実現され得ること、

本指令は、この目標の達成のために必要な程度を越え出てはいないこと、
以下の指令を制定した。

〔適用範囲〕

第１条　本指令の目的は、電子署名の利用を促進しかつその法的承認に資することである。本指令は、内部市場の真の機能の確保のために電子署名および特定の認証サービスのための法的枠組を設定する。

本指令は、国内法または共同体法により定められた形式に関する要件がある契約またはその他の法的義務の締結および有効性との関連での観点を把握するものでなく、国内法または共同体法において定められた文書の利用に関する規定および制限にも影響を与えない。

〔定義〕

第２条　本指令においては、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

１「電子署名」 別の電子データに付加されまたは論理的にそれと結びつけられておりかつ真正確認の方法として用いられる電子的形式のデータ

１「先進電子署名」 以下の要件を満たす電子署名

(a) それがもっぱら署名者のみに帰属させられており、

(b) 署名者の同一性確認が可能であり、

(c) 署名者がその唯一の統制の下に保持することのできる手段により作成されており、

(d) 事後的なデータの変更を認識させ得るように、その関連するデータにリンクされている。

３「署名者」 署名作成装置を所持しかつ自らの名前でか、またはそれが代表する機関または法人もしくは自然人の名前で行動する者

４「署名作成データ」 署名者により電子署名の作成のために利用されるコードまたは私的暗号キーのような唯一のデータ

５「署名作成装置」 署名作成データの具現のために利用される設定されたソフトウェアまたはハードウェア

６「安全署名作成装置」 付属書Ⅲの要求事項を満たす署名作成装置

７「署名検証データ」 電子署名の検証のために使われる、コードまたは公開暗号キーのようなデータ

８「署名検証装置」 署名検証データの具現のために使われる設定されたソフトウェアまたはハードウェア

９「証明証」ある者の署名検証データに関連させられかつその者の同一性を確認する電子的証明

１０「適格証明証」 付属書Ⅰに定める要求事項に適合する証明証を意味し、かつ付属書Ⅱに定める要求事項を充足する認証サービスプロバイダにより発行されているもの

１１「認証サービスプロバイダ」 証明証を発行しまたは電子署名に関連するその他のサービスを提供する機関または法人もしくは自然人

１２「電子署名製品」 認証サービスプロバイダにより電子署名サービスの提供のために利用されるよう意図された、または電子署名の作成または検証のために用いられることを意図されたハードウェアもしくはソフトウェアまたはそれらの一部

１３「任意認定(voluntary accreditation)」 特殊に認証サービスの提供のための権利および義務を課すあらゆる許認可で、当該認証サービスプロバイダの申請に基づいて与えられ、かかる権利および義務の細目を定めかつそれら権利義務の遵守を監督する権限を与えられた公共団体または私的団体により与えられるものを意味し、認証サービスプロバイダが当該許認可団体による決定を受けるまでは許認可から生じる権利を行使する資格が与えられない場合のそれ。

〔市場アクセス〕

第３条　構成国は、認証サービスの提供を事前の許認可にかからしめないものとする。

(2)　第一項の規定にかかわらず、構成国は認証サービス提供の水準強化を目標とする任意認定制度を導入しまたは維持することができる。かかる制度に関連するすべての条件は、客観的で、透明で、比例的でかつ無差別なものでなければならない。構成国は、本指令の適用範囲内に含まれる理由のために、認定認証サービスプロバイダの数を制限してはならない。

(3)　各構成国は、その領土内で設立され公に適格証明証を発行する認証サービスプロバイダの監督のための適切なシステムを構築することを確保するものとする。

(4)　付属書Ⅲに定める諸要求事項への安全署名作成装置の適合性は、構成国により指定された公共団体または私的団体により判定されるものとする。委員会は、第９条に定められた手続きにより、ある団体を指定するかどうかを構成国が決定するための基準を確立するものとする。

前段落で定められた機関によりなされた付属書Ⅲに定める要求事項との適合性の判定は、すべての構成国により承認されるものとする。

(5)　委員会は、第９条に定められた手続きにより、電子署名製品のための一般に承認された規格を確立しかつその参照番号を欧州共同体官報(Official Journal)において公示することができる。構成国は、電子署名製品がそれらの規格に適合するときは、付属書Ⅱ鋌項および付属書Ⅲに定める要求事項への適合があるものと推定するものとする。

(6)　構成国および委員会は、付属書Ⅳに定められた安全署名検査のための推奨事項に照らしてかつ消費者の利益のために署名検査装置の開発および利用を促進するために協力するものとする。

(7)　構成国は、公共部門における電子署名の利用をありうる付加的な要件に服さしめることができる。かかる要件は、客観的で、透明、比例的でかつ無差別なものとし、当該アプリケーションの特殊な性格にのみ関連しているものとする。かかる要件は、市民のための国境を越えたサービスに対する障害物となってはならない。

〔内部市場原則〕

第４条　各構成国は、その領土内で設立された認証サービスプロバイダおよびそれらが提供するサービスに、本指令にしたがって採用する国内規定を適用するものとする。構成国は、本指令の適用範囲内の分野において他の構成国に由来する認証サービスの提供を制限してはならない。

(2)　構成国は、本指令に適合する電子署名製品が自由に内部市場において流通することを許容されているよう確保するものとする。

〔電子署名の法的効果〕

第５条　構成国は、適格証明証に基づきかつ安全署名作成装置により作成された先進電子署名が、次の各号の条件をみたすよう確保するものとする。

(a)　手書き署名が紙ベースのデータに関連して求められる要件を満足するのと同様に、電子的形式でのデータに関して署名の法的要件を満足させること、および

(b)　法的な争訟手続において証拠として認められること。

(2)　構成国は、電子署名がもっぱら次の理由に基づいて法的効果および法的争訟手続きにおける証拠としての承認を否定されないことを確保するものとする。それが、

－　電子的形式をとっていること、または

－　適格証明証に基づいていないこと、または

－　認定認証サービスプロバイダによって発行された適格証明証に基づいていないこと、または

－　安全署名作成装置により作成されていないこと。

〔責任〕

第６条　最小限の事項として、構成国は、認証サービスプロバイダが、過失により行動していないことを証明するのでないかぎり、適格証明証として公に証明証を発行することによりまたはかかる証明証を公に保証することにより、その証明証を次の各号の点につき合理的に信頼するあらゆる機関または法人もしくは自然人に生じた損害を賠償する責任を負うことを、確保するものとする。

(a)　適格証明証に含まれているすべての情報の、証明証発行時における正確さに関して、および適格証明証に関して定められているすべての細目をその証明証が含んでいるという事実に関して。

(b)　証明証の発行時において、適格証明証において同一確認されている署名者が、証明証において与えられまたは同一確認されている署名検査データへの署名作成データの対応関係を保持していたということの保証について。

(c)　認証サービスプロバイダが署名作成データおよび署名検査データの双方を生成した場合においてそれらが相補的に使われることとができることの保証について。

(2)　最小限の事項として、構成国は、適格証明証として証明証を公に発行した認証サービスプロバイダが、それが過失により行動しなかったことを証明するのでない限り、証明証の取消の登録の過誤に関して、証明証を合理的に信頼する機関または法人もしくは自然人に生じた損害を賠償する責任を負うことを確保するものとする。

(3)　構成国は、認証サービスプロバイダが証明証の利用についての制限を、その制限が第三者に認識可能であれば、適格証明証に表示することができることを確保するものとする。認証サービスプロバイダは、証明証に付された制限を越える適格証明証の利用から生じる損害については責任を負わないものとする。

(4)　構成国は、認証サービスプロバイダが、証明証が使われ得る取引の価額についての限度を、その限度が第三者に認識可能であれば、適格証明証に表示することができることを確保する。

　認証サービスプロバイダは、この最高限度を越えたことによる損害については責任を負わないものとする。

(5)　第１項ないし第４項の規定は、消費者契約における不公正条項についての1993 年 4 月 5 日の理事会指令 93／13／EEC(1) には関わらないものとする。

(1)　OJ L 95, 21. 4. 1993, p. 29.

〔国際的観点〕

第７条　構成国は、第三国において設立された認証サービスプロバイダにより公に適格証明証として発行された証明証が、次の各号の条件をみたすときは、共同体内において設立された認証サービスプロバイダにより発行された証明証と法的に同等なものとして認められることを確保するものとする。

(a)　その認証サービスプロバイダが、本指令に定める要件をみたし、かつ構成国において制度化された任意認定制度のもとで認定されたものであること、または、

(b)　共同体内で設立された本指令に定められた要件をみたす認証サービス

プロバイダが、その証明証を保証していること、または、

(c) 共同体と第三国または国際組織の間で締結された二国間または多数国間条約のもとで証明証または認証サービスプロバイダが承認されていること。

(2) 第三国との国境を越えた認証サービスおよび第三国に由来する先進電子署名の法的承認の促進のために、委員会は、適切であれば、認証サービスに適用されうる規格および国際条約の効果的な実施を達成するための提案を行うものとする。特に、そして必要があれば、第三国および国際組織との二国間および多数国間条約の交渉のための適切な命令を理事会に提案するものとする。理事会は、特別多数でそれを決定するものとする。

(3) 委員会が、第三国における市場アクセスに関して共同体の企業になんらかの困難が生じていることを知ったときは、必要なときは、これら第三国における共同体の企業のための相当の権利の交渉のための適切な命令のために理事会に提案を行うことができる。理事会は、特別多数でそれを決定するものとする。

本項の規定にしたがい行われる措置は、関連する国際条約の下での共同体および構成国の義務には関わらないものとする。

〔データ保護〕

第８条 構成国は、認証サービスプロバイダおよび認定または監督の責任を負う国内機関が、個人データ処理に係る個人の保護およびかかるデータの自由な移動に関する 1995 年 10 月 24 日の欧州議会および理事会の指令 95／46／EC(2) に定められた要件を遵守することを確保するものとする。

(2) OJ L 281, 23. 11. 1995, p. 31.

(2) 構成国は、公に証明証を発行する認証サービスプロバイダが、データ主体から直接にのみ、またはデータ主体の明示的な同意を得た後に、および証明証の発行および管理の目的に必要な限りでのみ、個人データを収集することができることを確保するものとする。データは、データ主体の明示の同意なしには、その他のあらゆる目的のために収集されまたは処理されてはならない。

(3) 国内法の下で仮名に対して与えられた法的効果にかかわらず、構成国は、認証サービスプロバイダが証明証の中で署名者の氏名に代えて仮名を記載することを禁止しないものとする。

〔署名委員会(Committee)〕

第９条 委員会は、「電子署名委員会」(以下、署名委員会という)により補助されるものとする。

(2) 本項への参照については、1999／468／EC 決議の第八条の規定を考慮しつつ、同決議第４条および第七条を適用するものとする。1999／468／EC 決議の第４条第３項に定める期間は、3 カ月とする。

(3)　署名委員会は、手続きについてはそれ自身の規則を定めるものとする。

〔署名委員会の任務〕

第１０条　署名委員会は、本指令付属書に定める要求事項、第３条第４項にいう基準および第３条第５項にしたがい確立され公にされる電子署名製品のための一般に認められた規格を、第９条第２項に定める手続きにしたがい明確にするものとする。

〔通知〕

第１１条　構成国は、委員会およびその他の構成国に対して、次の各号について通知するものとする。

(a)　第３条第７項による付加的な要件を含めて、国内の任意的な認定制度についての情報

(b)　認定および監督の責務を負う国内機関の名称および所在地ならびに第３条第４項で定める機関

(c)　すべての国内認定認証サービスプロバイダの名称および所在地

(2)　構成国は、第１項の下で提供されるすべての情報およびその情報に関する変更を、可及的速やかに通知するものとする。

〔点検〕

第１２条　委員会は、遅くとも 2003 年 7 月 19 日までに、本指令の作用を点検し、そしてそれについて欧州議会および欧州理事会に対し報告するものとする。

(2)　点検は、技術的、市場的および法的発展を考慮しつつ、とりわけ、本指令の適用範囲が変更されるべきかどうかについて評価するものとする。報告は、特に、得られた経験に基づき整合化の観点からの評価を含むものとする。報告は、適切であれば、立法案を伴うものとする。

〔実施〕

第１３条　構成国は、本指令を遵守するために必要な法律、規則および行政規則を 2001 年 7 月 19 日以前に施行するものとする。構成国は、その点につきただちに委員会に情報提供するものとする。

構成国がこれらの措置を取るときは、これらの措置が本指令への参照条項を含むものとするか、またはそれらの公布に際してかかる参照を伴うものとする。かかる参照のしかたは、構成国がこれを定めるものとする。

(2)　構成国は、本指令により管理される分野において採用する国内法の主要規定の条文を委員会に連絡するものとする。

〔施行〕

第１４条　本指令は、欧州共同体官報へのその公布の日に施行するものとする。

〔名宛人〕

第１５条　本指令は、構成国をその名宛人とする。

1999 年 12 月 13 日
ブリュッセルにて
欧州議会議長　　N・フォンテーヌ
欧州理事会議長　　S・ハッシ

付属書Ⅰ　　適格証明証の要求事項

適格証明証は、次の各号を含まなければならない。

(a)　証明証が適格証明証として発行されたことの表示

(b)　認証サービスプロバイダおよびその設立された国の表示

(c)　同一確認されるべき署名者の氏名または仮名

(d)　証明証の意図された目的にかかわり、関連するものであれば含まれるべき、署名者の特殊な属性の条項

(e)　署名者の統制の下にある署名作成データに対応する署名検証データ

(f)　証明証の有効期間の始期と終期の表示

(g)　証明証の特定(ID)コード

(h)　証明証を発行する認証サービスプロバイダの先進電子署名

(i)　適用可能であれば、証明証の使用範囲についての限定、および

(j)　適用可能であれば、証明証が使われ得る目的となる取引の価額についての限定

付属書Ⅱ　　適格証明証を発行する認証サービスプロバイダの要求事項

認証サービスプロバイダは、次の各号の要件を満たさなければならない。

(a)　認証サービス提供に必要な信頼性を証明すること。

(b)　迅速かつ安全なディレクトリ操作および安全かつ即時の取消サービスの操作を確保すること。

(c)　証明証が発行されまたは取り消される日時が精確に決定され得ることを確保すること。

(d)　国内法により適切な手段により、適格証明証が発行される者の同一性および、適用可能な場合は、あらゆる特殊な属性を確認すること。

(e)　提供されるサービスに必要な専門知識、経験および資格を、特に管理者レベルの権限、電子署名技術の専門知識および妥当な安全手続きの熟練を、有する職員を雇用すること。それらは、証認された規格に対応する適切な管理的および運営的な手続を適用しなければならない。

(f)　変更から保護され、かつそれらによりサポートされるプロセスの技術的および暗号技術的なセキュリティを確保する信頼性のあるシステムおよび製品を使用すること。

(g)　証明証の偽造防止の措置をとること、および認証サービスプロバイダが署名作成データを生成する場合においては、かかるデータの生成プロセスにおける秘密

を保証すること。

(h)　本指令に定める要件に適合して活動するために十分な金銭的資源を維持すること、特に、損害賠償責任のリスクに耐えるために、たとえば適切な保険を付していることなどによる。

(i)　適切な期間、適格証明証に関するすべての関連情報を記録に留めること、特に、法的争訟手続を目的として証明の証拠を提供することを目的として。かかる記録は、電子的にこれを行うことができる。

(j)　認証サービスプロバイダがキー管理サービスを提供する者の署名作成データを保存または複写してはならないこと。

(k)　その電子署名の補助のために証明証を求める者との契約上の関係に入る前に、耐久的な通信手段によって、証明証の利用に関する制限、任意認定制度の存在および不服申立および紛争解決の手続きを含む、証明証の利用に関する精確な条件をその者に知らせること。電子的に伝達されてもよいかかる情報は、文書によりかつ容易に理解できる言語で与えられなければならない。この情報の関連部分は、証明証を信頼する第三者に対しても求めに応じて提供されなければならない。

(l)　検証可能な形式で証明証を保存するための、次の点を可能とする信頼性のあるシステムを用いること。

－　権原を与えられた者のみが登録および修正可能であること、

－　情報の真正性を点検し得ること、

－　証明証の保持者の同意が得られた場合にのみ証明証が公に取得可能となっていること、および

－　これらセキュリティ要件と妥協するあらゆる技術的な変更が、操作者に明かであること。

付属書III　　安全署名作成装置の要求事項

1．安全署名作成装置は、適切な技術的および手続的な手段によって、少なくとも次の各号を確保しなければならない。

(a)　署名の生成に利用される署名作成データが、実際上一回のみ作成され、かつその秘密が合理的に確保されていること、

(b)　署名の生成に利用される署名作成データが、合理的な保証のもとに、推定されることができず、かつ署名が現在利用可能な技術を用いた偽造から保護されていること、

(c)　署名の生成に利用される署名作成データが、他人の利用に対して、正当な署名者により確実に保護され得ること、

2．安全署名作成装置は、署名されるデータを変更してはならず、またはかかるデー

タが署名手続きの前に署名者に明らかにされることを禁じてはならない。

付属書IV　　安全署名検証についての推奨事項

署名検証プロセスに際し、合理的な確実性をもって、次の各号に定める事項が確保されたほうがよい。

(a)　署名検証のために使われるデータが、検証者に表示されるデータと対応していること、

(b)　署名が確実に検証され、かつその検証の結果が、正しく表示されること、

(c)　検証者が、必要に応じて、署名されたデータの内容を確実に確認することができること、

(d)　署名検証の時点で求められる証明証の真正性およびバリディティが、確実に検証されること、

(e)　検証の結果および署名者の同一性が正しく表示されること、

(f)　仮名の利用が明確に示されること、および、

(g)　あらゆるセキュリティに関連する変更が検出され得ること。

● 電子署名の大綱条件に関する法律(署名法 SigG)(2001 年 5 月 16 日)

(2001 年 5 月 16 日公布)

(Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften v. 16. 5. 2001, BGBl. I S. 876)

米丸恒治訳[57]

第１章　総則

〔目的および適用範囲〕

第１条　本法の目的は、電子署名についての大綱条件を創出することである。

(2)　特定の電子署名が法令により定められていない限りで、その利用は自由である。

(3)　公法上の行政活動に関しては、法令により、適格電子署名の利用に補足的な要件を付加することをさだめることができる。これの要件は客観的で、比例的かつ非差別的なものでなければならず、関連する利用の特殊な徴表のみに関連してもよい。

〔定義〕

第２条　本法においては、次の各号に定める表現は、当該各号に定めるところによる

1　「電子署名」別の電子データに付加されまたは論理的にそれと結びつけられており、かつ真正確認(Authentifizierung)のために用いられる電子的形式のデータ

2　「先進電子署名」前号による電子署名で、以下の要件を満たすもの

a)　それがもっぱら署名キー所持者のみに帰属させられており、

b)　署名キー所持者の同一性確認を可能にし、

c)　署名キー所持者がその唯一の統制のもとに保持することのできる手段により作成されており、

d)　事後的なデータの変更を認識させ得るように、その関連するデータに関連しているもの。

3　「適格電子署名」第２号による電子署名で、以下の要件を満たすもの

a)　その作成された時点で有効な適格証明証に基づいており、かつ

b)　安全署名作成装置により作成されたもの

4　「署名キー」電子署名の作成のために利用される私的暗号キーのような唯一の電子データ

5　「署名検査キー」電子署名の検証のために利用される公開暗号キーのような電子データ

---

[57] 新電子署名法の訳文は、米丸恒治訳「〔資料〕ドイツ新電子署名法」立命館法学 279 号 163-180 頁(2002 年)、同「〔資料〕ドイツ・マルチメディア法」多賀谷一照・松本恒雄編『情報ネットワークの法律実務』第一法規 7301-7326 頁(2002 年)所収のものを利用した。なお同書所収に際して校正時に修正した部分が、本資料においては反映されていない可能性があるため、正確には同書を参照していただきたい。

6　「証明証」署名検査キーがある者に属することおよびこの者の同一性を確認する電子的証明

7　「適格証明証」自然人のための第６号による電子的証明で、第７条の要件を満たしかつ少なくとも本法第４条ないし第１４条または第２３条およびそれに関連する第２４条による法規命令の規定の要件を満たす認証サービスプロバイダにより作成されたもの

8　「認証サービスプロバイダ」適格証明証または適格タイムスタンプを発行する自然人または法人

9　「署名キー所持者」署名キーを所有しており、かつそれに対する署名検査キーが適格証明証により帰属させられている自然人

10　「安全署名作成装置」　少なくとも本法第１７条または第２３条およびそれに関連する第２４条による法規命令の規定の要件を満たしかつ適格電子署名のために定められたそのつどの署名キーの保存および利用のためのソフトウェア装置またはハードウェア装置

11　「署名利用装置」次の事項のために定められたソフトウェア商品およびハードウェア商品

a)　適格電子署名の生成または検証のためのプロセスにデータを持ち込むためのものか、または

b)　適格電子署名を検証しもしくは適格証明証を検証し、そしてその結果を表示するためのもの

12　「認証サービスのための技術的装置」次の事項のために定められたソフトウェア商品またはハードウェア商品

a)　署名キーを生成しそして安全署名作成装置へと移転させるためのもの、

b)　適格証明証を公けに検証可能にしそして場合によっては呼び出し可能な状況に保ためのもの、または

c)　適格タイムスタンプを生成するためのもの

13　「適格電子署名商品」安全署名作成装置、署名利用装置および認証サービスのための技術的装置

14　「適格タイムスタンプ」少なくとも本法第４条ないし第１４条ならびに第１７条または本法第２３条およびそれに関連する、第２４条による法規命令の規定の要件を満たす認証サービスプロバイダの電子証明証であって、そのプロバイダに特定の電子データが特定の時点で提示されたことを示すもの

15　「任意認定」特別の権利および義務を伴う、認証サービス運営のための許可を付与するための手続

〔権限行政庁〕

第３条　本法および第２４条による法規命令による権限ある行政庁の任務は、電気通信

法第６６条による行政庁がこれを担当する義務を負う。

第２章　　認証サービスプロバイダ

〔一般要件〕

第４条　認証サービスの経営は、本法の枠内では、許認可不要である。

(2)　認証サービスは、その経営に必要な信頼性および専門知識ならびに第 12 条による補償の用意を証明し、かつ本法および第２４条第１号、第３号および第４号による法規命令による認証サービス経営のためのさらなる要件を満たすことを保証する者のみがこれを営むことができる。必要な信頼性は、認証サービスプロバイダとして経営の基準となる法令を遵守することについて保証をする者がこれを有する。必要な専門知識は、認証サービスの運営に携わる者がこの活動に必要な知識、経験および熟練を有するときに存在する。本法および第 24 条第１号、第３号および第４号による法規命令によるセキュリティ要件を実施するための措置を権限行政庁に対しセキュリティ計画で示しかつ適切かつ実際に実施に移すときには、認証サービスの運営のためのさらなる要件が存在する。

(3)　認証サービスの運営をはじめる者は、そのことを権限行政庁に対し遅くとも運営開始のときまでに届け出なければならない。届出とともに、第２項の要件が存在することを適当な形式で説明するものとする。

(4)　第２項による要件の充足は、認証サービスの活動の全期間にわたって確保されるものとする。もはやそれが不可能な事情があるときは、権限行政庁に対し、遅滞なく届け出るものとする。

(5)　認証サービスプロバイダは、第２項第４段によるセキュリティ計画に組み込んで、本法および第２４条による法規命令による任務を第三者に委任することができる。

〔適格証明証の付与〕

第５条　認証サービスプロバイダは、適格証明証を申請する者を信頼性をもって同一性確認しなければならない。プロバイダは、同一性確認された者に署名検証キーが帰属することを適格証明証によって証明しなければならず、かつこの証明証をいつでも何人に対しても公に到達可能な通信回線によって検証可能かつ呼び出し可能な状態にしておかなければならない。適格証明証は、署名キー所持者の同意を得てのみ呼び出し可能な状態にしておくことができる。

(2)　適格証明証には、申請者の求めに応じて、第三者のための代表権についての表示およびその者の職業に関連するかまたはその他の表示(属性)を含めることができる。代表権についての表示に関しては、その第三者の同意が示されるものとし、その者の職業に関連するかまたはその他の表示は、職業関連のまたはその他の表示の権限ある機関によって証明するものとする。第三者のための代表権についての表示は、第２段による同意が示されたときにのみ、その者につ

いての申請者の職業に関するかまたはその他の表示は、第２段による証明が示されたときにのみ適格証明証に取りいれることができる。その者に関するその他の表示は、関係者の同意があるときにのみ、適格証明証に取り込むことができる。

(3)　認証サービスプロバイダは、申請者の求めに応じて、適格証明証に、申請者の名前に代えて仮名を取り込まなければならない。適格証明証が、第三者のための代表権または職業関連もしくはその他のその者についての表示を含むときは、仮名の利用のためには、その第三者のまたは職業関連もしくはその他の表示について権限ある機関の承認を必要とする。

(4)　認証サービスプロバイダは、適格証明証のデータがきづかれずして偽造または変造されることができないような措置をとらなければならない。プロバイダは、署名キーが秘密に管理されることを担保するためのさらなる措置をとらなければならない。安全署名作成装置外での署名キーの保存は許されない。

(5)　認証サービスプロバイダは、認証活動の実施のために、少なくとも本法第４条ないし第１４条および第１７条または本法第２３条および第２４条による法規命令により信頼性のある職員および適格電子署名商品を用いなければならない。

(6)　認証サービスプロバイダは、申請者が付属の安全署名作成装置を所有していることを適切な方法で確信しなければならない。

〔教示義務〕

第６条　認証サービスプロバイダは、第５条第１項による申請者に対し、適格電子署名のセキュリティおよび信頼性のある検証に必要な諸措置について教示しなければならない。プロバイダは、申請者に対し、現存する署名の安全度が時間の経過により低下する前に、適格電子署名がなされたデータに必要に応じ新たに署名しなければならないことを指示しなければならない。

(2)　認証サービスプロバイダは、申請者に対し、法律に異なる定めのない限り、適格電子署名が法的取引において手書きの署名と同等の効果を有することを教示しなければならない。

(3)　第１項および第２項による教示のために、申請者に対しては、文書での教示を手渡さなければならない。それを了知したことを申請者は別途の署名で確認しなければならない。申請者が第１項および第２項よりもすでに早い時点で教示された限りでは、新たな教示はこれを行わないことができる。

〔適格証明証の内容〕

第７条　適格証明証は、次の各号の表示を含み、適格電子署名を有していなければならない。

１　署名キー所持者の氏名で、誤認される可能性がある場合は付随的な表示を付されたもの、または署名キー所持者に属する誤認され得ない仮名で仮名とし

てみわけのつくもの
2　付随する署名検証キー
3　署名キー所持者の署名検証キーおよび認証サービスプロバイダの署名検証キーが利用される際に使われるアルゴリズムの表示
4　証明証の通し番号
5　証明証の有効期間の始期と終期
6　認証サービスプロバイダの名称およびそれが営業所をおく国の名称
7　署名キーの利用が特定の利用方法または範囲に限定されるかどうかについての表示
8　適格証明証であることの表示
9　必要に応じ、署名キー所持者の属性

(2)　属性は、別途の適格証明証(適格属性証明証)に取り込むこともできる。適格属性証明証の場合には、第１項による表示は、適格属性証明証の利用に必要でない限りにおいて、それが関連する適格証明証の一義的な参照データによって代替することもできる。

〔適格証明証の停止〕

第８条　認証サービスプロバイダは、署名キー所持者またはその代理人が適格証明証の停止を求めるとき、証明証が第７条についての誤った情報に基づき作成されたものであるとき、認証サービスプロバイダがその活動を廃止しその活動がその他の認証サービスプロバイダにより継続されないとき、または権限行政庁が第１９条第４項に従いその停止を命ずるときは、適格証明証を遅滞なく停止しなければならない。停止措置には、停止措置の効力が生じる時点が含まれていなければならない。遡及的な停止は許されない。適格証明証が誤った表示をもって作成されたものであるときは、認証サービスプロバイダは、そのことを付加的に公表することができる。

(2)　適格証明証が第５条第２項による表示を含む場合は、その第三者またはその者の職業関連もしくはその者についてのその他の表示に権限を有する機関もまた、その者についての職業関連またはその他の表示についての要件が適格証明証へのその表示の取込み後に消滅したときは、第１項による当該証明証の停止を求めることができる。

〔適格タイムスタンプ〕

第９条　認証サービスプロバイダが適格タイムスタンプを発行するときは、第５条第５項を準用する。

〔記録〕

第１０条　認証サービスプロバイダは、本法および第２４条第１号、第３号および第４

号による法規命令を遵守するためのセキュリティ措置ならびに発行した適格証明証を第２段の規準により、そのデータおよびその改ざんされていないことがいつでも事後審査可能であるように記録しなければならない。記録は、遅滞なく、それが事後的に気づかれることなく変更されることができないようになされなければならない。これは、特に適格証明証の発行および停止について妥当する。

(2)　署名キー所持者に対しては、求めに応じてそれに関連するデータおよび手続段階を閲覧する機会が与えられなければならない。

〔責任〕

第１１条　認証サービスプロバイダが本法および第２４条による法規命令の要件に違反しまたはその適格電子署名商品もしくはその他の技術的なセキュリティ装置が機能しないときは、プロバイダは、適格証明証の表示、適格タイムスタンプまたは第５条第１項第２段による表示を信頼することにより損害を被った第三者の損害を賠償しなければならない。第三者がその表示の瑕疵あることを知っていたかまたは知らなければならなかったときは、補償義務は生じない。

(2)　認証サービスプロバイダが故意または過失により行動したものでないときは、補償義務は生じない。

(3)　適格証明証が署名キーの利用を特定の利用方法および範囲に限定しているときは、補償義務は、この限定の範囲内でのみ生じる。

(4)　認証サービスプロバイダは、第４条第５項による委託した第三者につきおよび第２３条第１項第２号による外国の証明証を保証したさいには、自らの行動についてと同様の賠償責任を負う。民法典第８３１条第１項第２段は、これを適用しない。

〔補償の用意〕

第１２条　認証サービスプロバイダは、それが本法または第２４条の法規命令の要件に違反しまたは適格電子署名商品もしくはその他の技術的セキュリティ設備が機能しないことによって生じる損害の賠償義務を果たすことのできる適切な保障の備えをなす義務を負う。最低額は、第１段に示された種類の原因の損害につき責任を生ぜしめる事故１件につきそれぞれ25万ユーロとする。

〔活動の停止〕

第１３条　認証サービスプロバイダは、その活動の停止については遅滞なく権限行政庁に届け出なければならない。プロバイダは、活動の停止の際に有効な適格証明証を他の認証サービスプロバイダに引き継がせるよう配慮するか、またはそれを停止しなければならない。プロバイダは、関係する署名キー所持者に、その活動の停止および他の認証サービスプロバイダによる適格証明証の引き継ぎについて通知しなければならない。

(2)　認証サービスプロバイダは、第１０条による記録を第１項により証明証を引き継いだ認証サービスプロバイダに引き渡さなければならない。他の認証サービスプロバイダが記録を引き受けないときは権限ある行政庁がこれを引き受けなければならない。権限ある行政庁は、正当な利益が存するときは、技術的に不当に過大な負担なしに可能なかぎりにおいて、第２段による記録の照会に応じる。

(3)　認証サービスプロバイダは、破産手続の開始の申請を権限行政庁に遅滞なく届け出なければならない。

〔データ保護〕

第１４条　認証サービスプロバイダは、個人関連データは、当該関係者自身から直接にのみおよび適格証明証の目的にとって必要な限りでのみ、これを取得することができる。第三者のもとでのデータの取得は、関係者の同意があるときにのみ許される。第１段に定める目的以外の目的のためには、そのデータは、本法がそれを許容しまたは関係者が同意したときにのみ、これを用いることができる。

(2)　仮名を用いた署名キー所持者の場合にあっては、認証サービスプロバイダは、犯罪または秩序違反の訴追のため、公共の安全と秩序に対する危険の防止のためまたは連邦および州の憲法保護行政機関、連邦諜報局、軍事諜報機関もしくは税務行政機関の法律上の任務の遂行に必要な限りにおいて、または、裁判所が係属中の手続の範囲内でそこで適用される規定の基準によりそれを命じる限りにおいて、そのキー所持者の同一性確認についてのデータを求めに応じて権限ある機関に提供しなければならない。それらの回答は、記録しておかなければならない。情報を求める行政機関は、仮名の暴露についての教示によって法律上の任務の遂行がもはや侵害されることがないかまたは署名キー所持者の教示に対する利益が重大であるときは、署名キー所持者に対し、仮名の暴露について教示しなければならない。

(3)　第２条第８項に定める認証サービスプロバイダ以外の者が、電子署名についての証明証を発行する限りにおいては、第１項および第２項を準用する。

第３章　任意認定

〔認証サービスプロバイダの任意認定〕

第１５条　認証サービスプロバイダは、申請に基づき、権限ある行政庁により認定させることができ、権限ある行政庁は認定に際して私的機関を利用することができる。認定は、認証サービスプロバイダが本法および第２４条による法規命令の規定を満足させていることを証明するときに与えるものとする。認定された認証サービスプロバイダは、権限ある行政庁の認定マークを得る。この認定マークにより、プロバイダの適格証明証に基づく適格電子署名(プロバイダ認定をと

もなう適格電子署名)についての包括的に検査された技術的および管理的なセキュリティの証明が表される。認定された認証サービスプロバイダは、認定認証サービスプロバイダとしての表示を行い、かつ法的取引および商取引において、証明されたセキュリティを援用することができる。

(2)　第１項の要件の充足については、第４条第２項第４段によるセキュリティ計画が、第１８条による機関によりその適正性および実際上の実施にわたって包括的に検査されかつ証明されなければならない。その検査および証明は、セキュリティ上重要な変更の後および定期的に繰り返されなければならない。

(3)　認定には、運営の開始に際しおよび運営中に本法および第２４条による法規命令による要件の充足を確保するために必要である限りにおいて、付款を付することができる。

(4)　本法および第２４条による法規命令による要件を充足しないときは、認定はこれを拒否するものとし、第１９条を準用する。

(5)　本法および第２４条による法規命令により生じる義務を履行しない場合または第４項による拒否理由が存する場合においては、権限行政庁は、認定を撤回するか、またはその理由がすでに認定時点で存在したときで第１９条第２項による措置によって成果が期待できないときは取消さなければならない。

(6)　認定の撤回もしくは取消の場合において、または認定認証サービスプロバイダの活動の停止の場合においては、権限行政庁は、別の認定認証サービスプロバイダによるその活動の引き継ぎをまたは署名キー所持者との契約の精算を確保しなければならない。破産手続の開始の申請がなされる場合も、その活動が継続されないときは、同様とする。別の認定認証サービスプロバイダが記録を第１３条第２項にしたがい引き継がないときは、権限行政庁がこれを引き継がなければならず、第１０条第１項第２段は、これを準用する。

(7)　適格電子署名商品にあっては、第１７条第１項ないし第３項の規定および第２４条による法規命令による要件の充足は、科学技術の水準に照らし十分に検査され、かつ第１８条による機関により証明されたものでなければならず、第１項第３段はこれを準用する。認定認証サービスプロバイダは、次の各号に定める事項を実施しなければならない。

1　その認証活動のためには､第１段により検査および証明された適格電子署名商品のみを利用すること

2　適格証明証は､証拠に基づき第１段により検査されかつ証明された安全署名作成装置を証拠に基づき所有する者についてのみ、発行すること

3　署名キー所持者に、第６条第１項の範囲内で第１段により検査されかつ証明された署名利用装置について教示すること

〔権限行政庁の証明証〕

第１６条　権限行政庁は、認定認証サービスプロバイダに対し、その活動に必要な適格証明証を発行する。認定認証サービスプロバイダによる適格証明証の発行についての規定は、権限行政庁にこれを準用する。認定認証サービスプロバイダがその活動を停止しまたはその認定が取消もしくは撤回されるときは、権限行政庁は、その発行した適格証明証を停止する。

(2)　権限行政庁は、次の各号に定める事項について、いつでも何人に対しても、公に到達し得る通信回線によって検査可能かつ呼び出し可能な状態にしておかなければならない。

1　認定認証サービスプロバイダの名称、所在地および通信回線

2　認定の撤回または取消

3　それにより発行された適格証明証およびその停止、ならびに

4　認定認証サービスプロバイダの運営の終了および禁止

(3)　必要に応じて、権限行政庁は、第１５条第７項による商品の自動的真正確認のために認証サービスプロバイダまたは製造者の必要とする電子的証明も発行する。

第４章　技術的セキュリティ

〔適格電子署名商品〕

第１７条　署名キーの保存および適格電子署名の生成のためには、署名の偽造および署名されたデータの改竄を信頼性をもって認識可能にしかつ署名キーの不正な利用から保護する安全署名作成装置を利用しなければならない。署名キーそれ自体が安全署名作成装置により生成されたときは、第３項第１号を準用する。

(2)　署名されたデータの表示のためには、適格電子署名の生成を予め一義的に示しどのデータに署名が関連しているかを確認させるところの署名利用装置を必要とする。署名されたデータの検証のためには、次の各号に定める事項を確認させる署名利用装置を必要とする。

1　どのデータに署名が関連しているか

2　署名されたデータが改変されていないかどうか

3　どの署名キー所持者に署名が属するものとされているか

4　署名が基礎とする適格証明証および付属の適格属性証明証がどのような内容を有するか

5　第５条第１項第２段による証明証の検証がどのような結果になるか

署名利用装置は、必要に応じ、署名されるべきまたは署名されたデータの内容も十分に認識させるものでなければならない。署名キー所持者は、かかる署名利用装置を利用するかまたはその他適切な、適格電子署名のセキュリティ確保措置を実施するものとする。

(3)　認証サービスのための技術的な装置は、次の各号に定める目的の諸対策がなされたものでなければならない。

1　署名キーの生成および移転に際し、署名キーの唯一性および秘密保持を担保するため、および安全署名作成装置外での記録を排除するため

2　第５条第１項第２段にしたがい検証可能にしまたは呼び出し可能な状態に保たれる適格証明証が、権限なく変更されおよび権限なく呼び出されることから保護するため

3　適格タイムスタンプの生成に際し、偽造および変造を排除するため

(4)　第１項および第３項第１号ならびに第２４条による法規命令による要件の充足は、第１８条による機関によって証明されなければならない。第２項ならびに第３項第２号および第３号の要件の充足については、適格電子署名商品の製造者の宣言で足りる。

〔検査機関および証明機関の承認〕

第１８条　権限行政庁は、自然人または法人が、その活動に必要な信頼性、独立性および専門知識を証明するときは、その申請に基づき、それらを第１７条第４項もしくは第１５条第７項第１段による証明機関または第１５条第２項による検査機関および証明機関として、承認する。その承認には、内容的な制限を付し、それを暫定的なものとしもしくは一定の期限を定め、または負担を付して、それを行うことができる。

(2)　第１項により承認された機関は、その任務を、中立に、指揮命令から独立してかつ良心に従い実施しなければならない。その機関は、検査および証明を記録しなければならず、その活動を中止する場合においては記録を権限行政庁に引き渡さなければならない。

第５章　監督

〔監督措置〕

第１９条　本法および第２４条による法規命令の遵守についての監督は権限行政庁がこれを行うものとし、権限行政庁は監督の実施に際し私的機関を利用することができる。運営の開始とともに、認証サービスプロバイダは、権限行政庁の監督に服する。

(2)　権限行政庁は、認証サービスプロバイダに対して、本法および第２４条による法規命令の遵守を確保するために必要な措置を実施することができる。

(3)　権限行政庁は、次の各号の事項を正当化する事実があるときで第２項による措置では成果が期待できないときは、認証サービスプロバイダに対しその運営を一時的に、一部または全部禁止しなければならない。

1　プロバイダが、認証サービスの運営に必要な信頼性を有しないこと。

2　プロバイダが、運営のために必要な専門知識を有していることを証明しない

こと。

3　プロバイダが、必要な補償の用意をしていないこと。

4　プロバイダが、不適切な適格電子署名商品を利用していること。

5　プロバイダが、本法および第２４条による法規命令による認証サービスの運営のためのその他の要件を満たしていないこと。

(4)　権限行政庁は、適格証明証が偽造されもしくは十分に偽造に対し安全でないことまたは適格電子署名が気づかれずして偽造されることもしくはそれにより署名されたデータが気づかれずして変造されることを許容するセキュリティの欠陥を安全署名作成装置が示すことを正当化する事実があるときは、適格証明証の停止を命じることができる。

(5)　認証サービスプロバイダにより発行された適格証明証の有効性は、運営の禁止および活動の中止ならびに認定の取消および撤回により影響を受けない。

(6)　権限行政庁は、それに対し届出をした認証サービスプロバイダならびにその活動を第１３条により中止したまたはその運営を第１９条第３項により禁止された認証サービスプロバイダの名称を、なにびとに対しても公に到達し得る通信回線を通じて呼び出し可能な状態にしておかなければならない。

〔協力義務〕

第２０条　認証サービスうプロバイダおよびそのために第４条第５項により活動する第三者は、権限行政庁およびその委託を受けて行動する者に対し、通常の営業時間内に事業所および営業所への立入を許容し、求めに応じて必要な書籍、記録、証拠、書類およびその他の資料を適切な方法で閲覧に供し、またそれらが電子的形式で実施されているときは回答を与えかつ必要な援助を与えなければならない。

(2)　回答を与える義務を負う者は、それが回答を与えることによりそれ自身または民事訴訟法第３８３条第１項第１号ないし第３号に示された所属者の１が犯罪または秩序違反法による手続の対象とされるときは、回答を拒むことができる。この義務を負う者に対しては、この権利が示さなければならない。

第６章　補則

〔過料規定〕

第２１条　故意または過失により次の各号の１に該当する者は、秩序違反にあたる。

1　第２４条第１号､第３号および第４号による法規命令もあわせて第４条第２項第１段に違反して認証サービスを営む者

2　第４条第３項第１段または第１３条第１項第１段に違反して、届出を怠り、正しく行わず、または適時に行わなかった者

3　第２４条第１号による法規命令とあわせて第５条第１項第１段に違反して、

人物の同一性確認をせず、正しく行わず、または適時に行わない者

4　第２４条第１号による法規命令もあわせて第５条第１項第２段に違反して、適格証明証を検証可能な状態に保たない者

5　第５条第１項第３段に違反して、適格証明証を呼び出し可能な状態に保つ者

6　第５条第２項第３段または第４段に違反して、適格証明証の中に表示を取り入れる者

7　第２４条第１号による法規命令もあわせて第５条第４項第２段に違反して、措置を行わないかまたは正しく行わない者

8　第５条第４項第３段に違反して、署名キーを保存する者

9　第２４条第１号による法規命令もあわせて第１０条第１項第１段に違反して、セキュリティ措置または適格証明証を記録しないか、正しくもしくは適時に行わない者

10　第２４条第１号による法規命令もあわせて第１３条第１項第２段に違反して、適格証明証が他の認証サービスプロバイダにより引き継がれるよう配慮しない者、ならびに適格証明証を停止しないかまたは適時にしない者

11　第２４条第１号による法規命令とあわせて第１３条第１項第３段に違反して、署名キー所持者に教示をしないか、正しくもしくは適時に教示をしない者

(2)　第１項第１号、第７号および第８号の秩序違反にあっては、５万ユーロ以下の過料を、その他の秩序違反にあっては、１万ユーロ以下の過料を課すことができる。

(3)　秩序違反法第３６条第１項第１号の意味の行政庁は、電気通信郵便規制庁(Regulierungsbehörde für Telekommunikation und Post)である。

〔費用および負担金〕

第２２条　権限行政庁は、次の各号の職務活動について、費用(手数料および立替金)を徴収する。

1　第１５条および第２４条による法規命令による、認証サービスプロバイダの任意認定の範囲内での措置

2　第１６条第１項による適格証明証の作成および第１６条第３項による証明の作成の範囲内での措置

3　第１８条および第２４条による法規命令による検査機関および証明機関の承認の範囲内での措置

4　第４条第２項ないし第４項と合わせた第１９条第１項ないし第４項および第２４条による法規命令による監督の範囲内での措置

費用は、行政庁が監督の実施に際して私的機関を利用することにより生じる

行政費用についても徴収する。行政費用法は、これを適用する。

(2)　第４条第３項により運営を届け出た認証サービスプロバイダは、第１９条第６項による要件の継続的な充足のための行政費用支出を賄うために年度負担金として徴収される公課(Abgabe)を権限行政庁に支払わなければならない。第１５条第１項により認定されている認証サービスプロバイダは、第１６条第２項による要件の継続的な充足のための行政費用支出を賄うために、年度負担金として徴収される公課(Abgabe)を権限行政庁に支払わなければならない。

〔外国の電子署名および電子署名商品〕

第２３条　欧州連合の他の構成国またはその他の欧州経済圏条約の加盟国から発せられた外国の適格証明証が存在する電子署名は、それが現行の電子署名のための共同体の共通枠組に関する欧州議会および理事会の指令 1999/93/EC(ABl. EG 2000 Nr. L 13 S. 2)第５条第１項に対応するものである限り、適格電子署名と同様の取り扱いとする。第三国から発せられた電子署名は、当該国の認証サービスプロバイダの証明証が公に適格証明証として発行したものであり指令 1999/93/EC 第５条第１項の意味における電子署名のために定められたものでありかつ次の各号の１に該当するときは、適格電子署名と同様の取り扱いとする。

1　認証サービスプロバイダが、指令の要件を満たしかつ欧州連合の構成国またはその他の欧州経済圏条約の加盟国において認定を受けていること、

2　指令の要件を満たす、欧州共同体内に本拠地をおく認証サービスプロバイダがその証明証を保証していること、または

3　欧州連合と第三国間または国際機関間での二極間または他極間の協定の枠内で、証明証または認証サービスプロバイダが承認されていること

(2)　第１項による電子署名は、その同等のセキュリティが証拠により証明されるときは、第１５条第１項によるプロバイダの認定をともなう適格電子署名と同様の取り扱いとする。

(3)　欧州連合の構成国またはその他の欧州経済圏条約の加盟国において、現行の指令 1999/93/EC の要件に対応していることが確認された電子署名商品は、承認される。第１段に定める国または第三国からの電子署名商品は、それが同等のセキュリティを証拠により証明されるときは、第１５条第７項により検査された適格電子署名商品と、同様の取り扱いとする。

〔法規命令〕

第２４条　連邦政府は、第３条ないし第２３条の規定の実施のために必要な、次の各号についての法令を法規命令により発する権限を有する。

1　第４条第２項および第３項、第５条、第６条第１項、第８条、第１０条、第１３条および第１５条による、認証サービスプロバイダの運営開始および運営

中ならびに運営の中止に関しての義務の細目規定

2　手数料義務の要件および手数料額ならびに負担金の額および権限行政庁による負担金徴収の手続について、なお負担金額の積算に際しては、手数料によって賄われない限りでの行政費用支出(人的および物的支出)を根拠としなければならない。

3　第７条による適格証明証の内容の細目規定および有効期間

4　第１２条による補償の用意の義務の履行のために許容される担保給付およびその範囲、額および内容的な細目

5　第１７条第１項ないし第３項による適格電子署名商品、ならびに第１７条第４項および第１５条第７項による、要件を満たしていることの本商品の検査および証明についての細目要件

6　第１８条による検査機関および証明機関の承認手続および活動の細目

7　第６条第１項第２段により適格電子署名を付されたデータに新たに署名がなされなければならないものとされる期間およびその手続

8　第２３条による外国の電子署名および外国の電子署名商品の同等のセキュリティを確認するための手続

〔経過規定〕

第２５条　1998 年 12 月 19 日の法律(BGBl. Ⅰ S. 3836)第５条により改正された 1997 年 7 月 22 日の署名法(BGBl. I S. 1870, 1872)により免許を与えられた認証機関は、第１５条の意味で認定されているものとみなす。この認証機関は、本法の施行後 3 月以内に権限行政庁に対し第１２条による補償証明を提出しなければならない。

(2)　第 1 項による認証機関により、本法の施行のときまでに、1998 年 12 月 19 日の法律(BGBl. Ⅰ S. 3836)第５条により改正された 1997 年 7 月 28 日の署名法(BGBl. I S. 1870, 1872)第５条により発行された証明証は、適格証明証と同様の取り扱いとする。第１段による証明証の所持者は、本法施行後 6 月以内に第６条第２項により適切な方法で教示を与えられなければならない。

(3)　1998 年 12 月 19 日の法律(BGBl. I S. 3836)第５条により改正された 1997 年 7 月 22 日の署名法(BGBl. Ⅰ S. 1870, 1872)の第４条第３項第３段および第１４条第４項により権限行政庁によりなされた検査機関および証明機関の承認は、それが本法第１８条に適合する限りで、効力を有する。

(4)　1997 年 7 月 22 日の署名法(BGBl. Ⅰ S. 1870, 1872)の第１４条第４項による要件の充足が検査されかつ証明された技術的装置は、本法第１５条第７項による適格電子署名商品と同様の取り扱いとする。」

電子署名に関する命令（署名令）（新署名令）　2001 年 11 月 16 日　　〔抄訳〕

米丸恒治訳

（Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001, BGBl. I S. 3074）

Inhaltsübersicht

§ 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

(第 15 条　適格電子署名のための製品の要求事項)

(3) Technische Komponenten nach § 17 Abs. 3 des Signaturgesetzes müssen gewährleisten, dass die Sperrung eines qualifizierten Zertifikates nicht unbemerkt rückgängig gemacht werden kann und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte nach Satz 1 müssen beinhalten, ob die nachgeprüften qualifizierten Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren. Nur nachprüfbar gehaltene qualifizierte Zertifikate dürfen nicht öffentlich abrufbar sein. Im Falle des § 17 Abs. 3 Nr. 3 des Signaturgesetzes muss gewährleistet sein, dass die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird. (第３項　……（中略）……署名法第１７条第３項第３号の場合においては、適格タイムスタンプの生成のときに妥当する法律上の時を、改竄されることなく、タイムスタンプに取り込むことが確保されていなければならない。)

§ 17 Zeitraum und Verfahren zur langfristigen Datensicherung
(第 17 条　長期的なデータ確保のための期間および手続)

Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

(適格電子署名を有するデータは、これを、その生成および検証のために用いられたアルゴリズムおよび付属のパラメータが適切であると判断される(期間)よりも長期間にわたり署名された形式で保つ必要があるときは、署名法第６条第１項第２段により、これに新たに署名するものとする。この場合においては、データには、そのアルゴリズムまたは付属のパラメータの適性が消失する時点よりも前に､新たな適格電子署名を付するものとする。新適格電子署名は、適切な、新たなアルゴリズムまたは付属のパラメータを用いてこれを行わなければならず、以前の署名を含み、かつ適格タイムスタンプを付さなければならない。)

【連絡先】

タイムビジネス推進協議会（ＴＢＦ）
〒160-0022
東京都新宿区新宿 1-20-2　小池ビル
財団法人テレコム先端技術研究支援センター
タイムビジネス推進協議会事務局
Tel.03-3351-8423　　Fax.03-3351-6690
URL：http://www.scat.or.jo/time/