国内および海外における
タイムビジネスに関する調査
報告書

平成１７年５月

タイムビジネス推進協議会

目　次

１．はじめに

企画部会調査研究分科会では、タイムビジネスに関する調査および研究、情報の収集や提供、関係機関との連絡調整等を目的とした活動を行っている。本報告書では調査研究分科会が平成 16 年度に実施した国内外の調査等の活動について報告する。

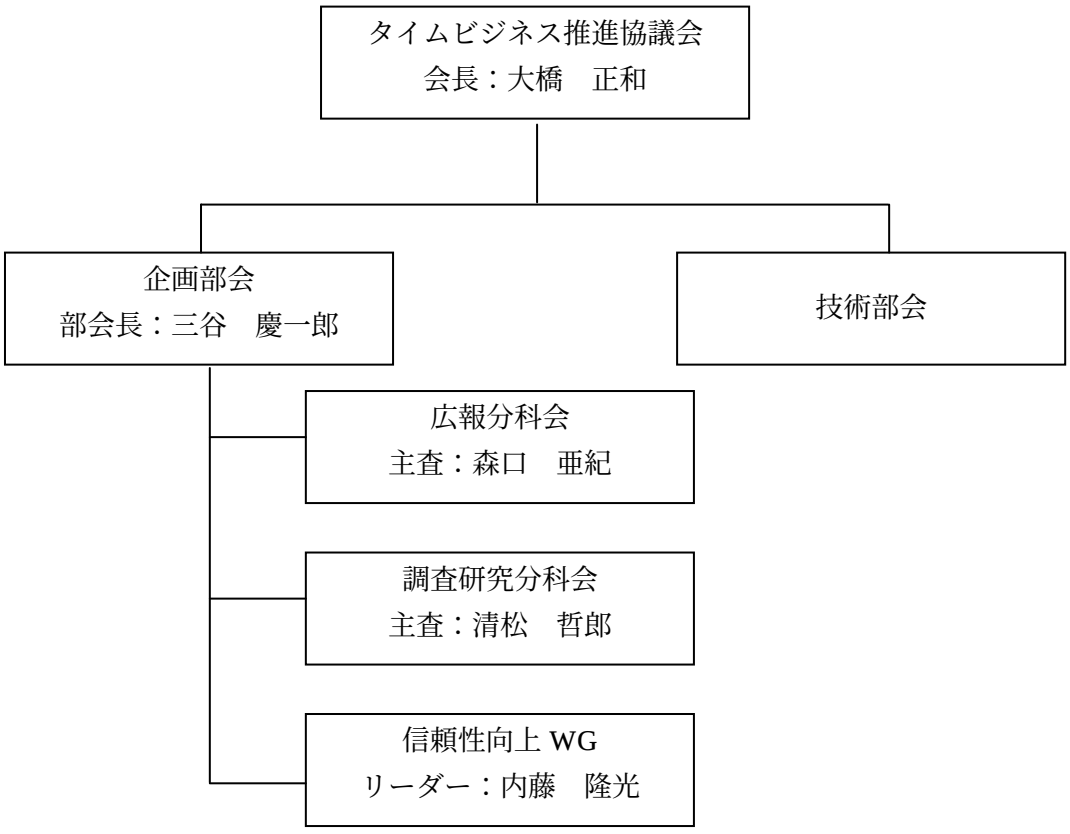
１．１　背景と目的

e－Japan 重点計画 2004 により、IT 規制改革の推進による情報技術の進展を踏まえて文書・帳票の真実性・可読性を確保しつつ電子保存を可能とする、いわゆる e-文書法の検討が平成 16 年に始まった。様々な場面で電子データの信頼性、正確性を確保することがますます重要となり、真正性を確保するためのタイムスタンプへの期待が高まった。

本調査では、そういった状況を背景として国内各分野におけるタイムスタンプの認識および動向、また海外における制度やサービス状況を調査して、今後のその発展方向および将来動向を予測し、タイムビジネスの健全な発展に資することを目的とする。

１．２　調査研究分科会体制

タイムビジネス推進協議会における調査研究分科会の位置付けを次に示す。



調査研究分科会のメンバー一覧を次に示す。

主査	清松　哲郎	株式会社日立製作所
	岩間　司	独立行政法人通信総合研究所
	臼杵　稔	横浜著作権研究会
	内田　斉	アライド・ブレインズ株式会社
	小島　英揮	アドビシステムズ株式会社
	小原　茂樹	pe-com
	木元　長憲	ＮＴＴコミュニケーションズ株式会社
	藤井　俊行	西日本電信電話株式会社
	酒井　雅啓	日本電気株式会社
	佐藤　忠弘	アマノ株式会社
	野口　隆弘	株式会社ＰＦＵ
	牧野　兼明	株式会社ＮＴＴデータ
	田邉　俊史	株式会社ＮＴＴデータ経営研究所
	廣瀬　智康	丸文株式会社
	三谷　慶一郎	株式会社ＮＴＴデータ経営研究所
	宮崎　豊	株式会社日立製作所
	松崎　秀雄	キヤノン販売株式会社
	西山　晃	セコムトラストネット株式会社

１．３　分科会の活動概要

分科会では、タイムスタンプに関する国内の状況調査活動および海外の状況調査活動を行った。国内調査活動としては国内各業界を代表する組織と意見交換会を行い、各分野におけるタイムスタンプに関する認識の程度、およびタイムスタンプの応用性や動向について調査した。海外の状況調査活動としては海外調査会社を利用した調査、および分科会独自にベンダのヒアリング調査を行った。

２．タイムビジネスに関する国内分野の状況

２．１　調査目的

各業界あるいは各分野における時刻配信およびタイムスタンプ等のタイムビジネスの認識の程度、および業界の有する背景や課題等を把握するとともに、タイムビジネスに関する今後の動向を予測する。

２．２　実施方法

e-文書法によって影響を受ける代表的な法律の例をピックアップし、その法律が対象とする分野について、その分野を代表する組織とコンタクトを取り、意見交換会を実施した。

e-文書法によって影響を受ける法律の例としてピックアップした法律を表 2.1 に示す。

表　２．１　e-文書方の対象法律（例）と分野

e-文書法の対象法律（例）	分野
証券取引法	金融・証券関連
投資信託及び投資法人に関する法律	
外国証券業者に関する法律	
株券等の保管及び振替に関する法律	
銀行法	
保険業法	
建設業法	建設関連
宅地建物取引業法	
建築基準法	
電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律	税務関連
医師法	医療関連
歯科医師法	
保健師助産師看護師法	
医療法	
著作権等管理事業法	知的財産権関連

上記の分野について検討を行い、タイムスタンプのニーズが大きいと思われる下記の分野を特定した。

その上で、各分野の複数の代表組織にコンタクトして、意見交換会を実施した。

（1）金融・証券関連
（2）税務関連
（3）建設関連
（4）医療関連
（5）知的財産権関連
（6）その他の分野

２．３　各分野における状況および動向

実施した意見交換会を通して得られた情報に加えて、一般的な情報を補完してそれぞれの分野の状況および動向を報告する。

２．３．１　金融・証券関連分野

業界の個々の企業では e-文書法による保存文書の電子化を意識していると思えるが、業界団体全体としての纏まった声としては、影響あるいは対応についての意見は特にない。

e-文書法は規制緩和であるので電子化しなければならないというものではなく、企業にとってはこれまで紙で保存していた文書を電子化して保存する明確なメリットがない限り、電子保存に切替える理由は見つからない。保存・保管だけを考えた場合、紙をスキャンして電子データとして保存することは、保管面積・体積の減少によるコストダウンがスキャン作業および機器の初期投資・運用費用等のコストを上回るのでなければ、電子化するメリットにはならない。その他のメリットとして、例えば参照が多い場合は検索性の向上や、ネットワークによって地理的制約から開放されるなどが挙げられる。

企業において検索のために既に文書等の電子化が済んでおり、一方で単なる法制による保管義務だけのために紙を保存していたのであれば、紙を破棄できるのでメリットは大きい。また、米国の 2001 年 9 月 11 日の同時多発テロ事件では、いち早くビジネスを再開できた会社は文書を電子化し、分散管理するなどして災害に備えていた企業である。文書の電子化はビジネス継続性の観点からもメリットがある。

企業には、e-文書法で電子保存が認められたからといって、これまで紙で保存していた文書をスキャンして電子化するのでは企業にとってのメリットは少なく、むしろ全体のワークフローの電子化と一緒に考えなければならない問題であるとの認識がある。電子保存の普及は大量に紙を扱う、電子保存による費用対効果の大きい企業から始まり、徐々に広がっていくと期待される。

２．３．２　税務関連分野

意見交換を実施した業界団体では、委員会メンバーがタイムビジネス推進協議会にも参加しており、e-文書法関連についてよく把握していたため、詳細にわたる深い議論が為された。

領収書について 3 万円以上のものは電子保存が認められない、あるいはカラーデータでの保存を要求するなど、要件が厳しいためにその対応システムの費用対効果を疑問視する声もある。しかし納税関連書類では企業の規模に関わらず、小さな企業であっても文書の保存スペースが少なくなるため、システムのコストにもよるが電子保存のメリットは見出せるという見解もあり、そういったニーズに応えるシステムが登場して幅広く普及することが考えられる。

２．３．３　建設関連分野

IT 書面一括法によって認められた建設工事の請負の電子入札・電子申請への対応など、業界として電子化への意識レベルは高い。国土交通省のガイドラインがあり、電子署名による原本性確保等を要求している。業界ではそういった応用分野でのタイムスタンプの必要性を理解している。e-文書法が対照としている文書の電子保存という分野を中心とするのではなく、電子入札や電子申請という分野でのタイムスタンプの応用が期待される。

２．３．４　医療関連分野

医療分野としては、カルテ、レセプト、紹介状、処方箋等の IT 化の推進が期待されている。また e-文書法は医療分野もカバーしており、これまで紙で保存していたカルテ等もスキャンしてデジタルデータとして電子保存することを認めている。

カルテについてはそのデジタル化、つまり電子カルテについて、既に従来から多くの議論および検討が行われている。カルテは長期にわたり保存される情報である。法定保存年限は５年であるが、個人の診療記録としてその個人の一生にわたって保存すべきであるとの意見もある。

電子カルテの検討では、その信頼性を得るために原本性確保の問題が議論されている。電子保存する場合に満たされなければならない規準として、真正性の確保、見読性の確保、保存性の確保が従来より示されている。電子カルテ検討の報告書では、改ざん検出にタイムスタンプがその機能を果たし、結果的に改ざん防止につながることが既に報告されており、実証実験システムや一部のシステムではタイムスタンプを用いて真正性を確保することを実現している。2005 年に公開された医療情報システムに関する安全管理についてのガイドラインでは、電子カルテに電子署名とタイムスタンプを付与することとしている。

レセプト処理については、その発行処理は IT 化されているが、請求処理はまだ紙が殆どである。今後は電子レセプトを前提としたオンライン請求の普及のための対応が始まり、

電子カルテと同様にその信頼性確保および証拠性確保のためにタイムスタンプの活用が期待される。

なお、処方箋の処理において発行処理はレセプト処理と同様に IT 化されているが、医局と薬局を結ぶオンライン化は、海外ではすでに実現されているところもあるが、国内ではまだ未解決の課題があるとされて実現していない。近い将来に処方箋もレセプトと同様に処理全体がデジタル化されてオンライン化が進み、その信頼性確保および証拠性確保のために電子署名とタイムスタンプが利用されることが期待される。

医療分野では IT 化に伴い、デジタルデータの信頼性確保に電子署名の仕掛けが必須と認識されて、医療における公開鍵基盤（HPKI）の整備が進んでいる。発行する医療機関や医師の証明書に基づく電子署名およびタイムスタンプにより、医療機関の間で受け渡される紹介状の他、電子カルテ、レセプト、処方箋等の情報の信頼性確保、証拠性確保が統一的に実現されていくと期待される。

医療分野での IT 化推進については、2001 年の「保健医療分野の情報化に向けてのグランドデザイン」、あるいは 2004 年 6 月に政府が発表した e-Japan 重点計画-2004 で 2004 年度までに全国の病院の 50%以上、2006 年度までに全国の病院の 70%以上においての IT 化の普及を目標としている。電子カルテの普及については e-Japan 重点計画-2004 で 2006 年度までに 400 床以上の病院および全診療所の 60%以上を目標としている。

大病院においては一日に数千人におよぶ外来患者が訪れる。その検査や診断結果の全てにタイムスタンプが適用されるとすると、そのタイムスタンプの数は莫大となる。病院および診療所の大幅な IT 化の目標達成に向けて今後具体的な措置が策定され、医療分野での IT 化が普及促進されていくと、それに伴いタイムスタンプが急速に普及していくことが期待される。

タイムスタンプの必要性の認識と大きな需要予測がある一方では、課題の指摘もあった。大量のタイムスタンプの付与に要するコストの問題、システムからより簡単にタイムスタンプが利用できるような仕掛けが必要であること、医療というクリティカルな分野での応用であるためにサービス停止が許されないこと、また大量な要求に対して処理が滞らないことなどが課題として挙げられた。

２．３．５　知的財産権関連分野

新製品の開発では新しい技術に関して数多くの発明が行われ、デザイナーは製品の意匠を数多くデザインする。インターネット社会でコンテンツと呼ばれる音楽や映像、画像の膨大なデータは著作権で保護される重要な知的財産である。特許・商標や著作権といった知的財産の分野では様々な係争が想定され、それに備えることが重要課題である。

特許等に関連する発明に関わる企業の日頃の研究開発あるいは意匠デザイン等も、この頃はコンピュータシステムの利用に頼っており、関連する情報はデジタルデータとして生成・保存されていると言っても過言ではない状況である。また最近の医薬開発や遺伝子工学に関する発明等はコンピュータによる膨大なデータの処理に頼っている。タイムスタン

プを付与し、デジタルデータの証拠性を確保して保存する意義は大きい。特に米国の特許制度は先発明主義をとっているために、発明の時点を特定するための内部書類､研究ノート､日誌、設計図面等にタイムスタンプを付与するという例があり、国内においても米国特許での係争に備えるためには同様に将来証拠となる可能性のある文書にタイムスタンプを付与することが有効であると考えられている。

音楽や映像の創作でもコンピュータシステムの利用に頼ることが多くなっており、著作物はデジタルデータとして生成され、電子保存されていることが多くなっている。プログラムやマニュアルと言った著作物は殆んど例外なくコンピュータシステムで作成・保存されている。文筆業を営む人々も作品をワープロで作成して、デジタル的に出版社に渡すなど、デジタル化が普及している。知的所有権の係争が発生した場合には、原告および被告の両者の知的所有物が創生された時点の前後関係の証明が重要である。そのため、各種文書や情報の作成された時点が重要な意味を持つ知的財産ではタイムスタンプの持つ時刻証明機能の意義は大きく、知的財産権分野での利用が進むと思われる。

２．３．６　その他の分野

紙による保存に代えて、技術的に確立されているマイクロフィルムによる保存が法律によって認められている文書は多い。そういった文書を保存するのに、これまで企業ではマイクロフィルムを採用する場合が多かったが、次世代では IT 化の流れを受けて文書を電子化して保存することを想定し、業界団体ではそのために必要な技術を検討してきている。また、変更の簡単な電子データに対して原本性確保等の証拠性を持たせるためには、電子署名やタイムスタンプが必要であることを従来からの検討で認識している。業界として e-文書法に対応した電子化に対応していくために、業界の各企業では電子署名およびタイムスタンプを利用できる環境整備を推進している。

さらに新しい分野としては、IT 化された社会において発生する様々な訴訟に対応できるようにコンピュータシステム上で証拠を確保して準備するというコンピュータフォーレンジックが最近になって注目を浴びている。2005 年 4 月に完全施行された個人情報保護法等により、コンピュータの不正アクセスや不正利用による情報漏洩から個人情報を守ることがさらに重要になってきている。コンピュータの不正アクセスや不正利用の発見には、コンピュータシステム上で採取される様々な記録が利用される。訴訟となった場合、その記録が証拠となるが、法廷での証拠とするためにはその記録自身が改ざんされていないことの証明と時刻の証明が重要になる。電子取引記録、電子メール等の各種データについても同様で、証拠として扱われる可能性が高まっており、タイムスタンプを付与して保存することは有効である。

インターネットの普及に伴って設置されたヘルプデスク、電話取引や製品への問合せ・苦情等を扱うコールセンタ等での電話による対応内容も、訴訟での証拠として扱われることがある。現在ヘルプデスクやコールセンタではで電話の会話内容もデジタル化して保存されている場合が多く、タイムスタンプを適用して証拠性を確保することができる。映像

による監視にも同様にタイムスタンプの適用等が考えられる。

また、文書の法的な証拠能力確保に関するサービスとして、法務大臣が任命した公証人が遺言や重要な契約文書の公正証書を作成したり、署名や記名捺印された文書の存在した日付の公の証明のために確定日付印を押印するというサービスがある。こういったサービスを行う公証役場の一部では、デジタル化された文書も同様に取り扱っている。このようなサービスは現在の社会で非常に重要な役目を担っており、IT 化が進む現代社会のニーズに応えて発展することが期待される。

例えばネットワーク上での仮想のデジタル公証役場等でタイムスタンプを活用して、デジタルデータの証拠性を高めるサービスなども考えられる。また従来から郵便局が行っている内容証明郵便というサービスがあり、後日相手に送付した法的な証拠として準備するために利用されることが多い。電子メールが普及した現代では同様のメール内容証明サービスも将来期待される。

今後は様々な問題解決の手段として訴訟が普通の手段となって行く可能性が高く、社会の IT 化の進展に伴い、訴訟で扱われる証拠も様々なデジタルデータである可能性がますます高まることが予想される。タイムスタンプを付与してデジタルデータを保存することは訴訟への準備という観点からも非常に有効であり、利用が広がると考えられる。

２．４　国内状況のまとめ

IT 化の進展に伴い電子データへの依存度が高まり、デジタルデータは従から主の立場に変わりつつある。そのデジタルデータの証拠性をどのように確保すべきかを以前から検討を重ねてきている分野もあり、そうした分野ではタイムスタンプに関してその必要性がはっきりと認識されている。しかし各分野でのタイムスタンプの認識については、それぞれの分野によってかなり差がある。また、検討が進んでいる分野では、タイムスタンプについて、その使い勝手や大量に使用する場合のコストや可用性・性能といった課題の指摘もあり、提供側の努力を望む声もあった。

医療分野ではタイムスタンプの必要性の認識が高く、IT 化が進んだ場合には大量のタイムスタンプが利用されると予測される。知的財産権分野では、係争への準備において発明や創作といった活動がなされた時点の証明が重要であり、タイムスタンプへの期待が大きい。

その他の広い分野で、トレーサビリティ向上や証拠性の確保という観点から、様々な記録データにタイムスタンプが付与されていくことが予測される。

今後解決していかなければならない課題はあるが、タイムスタンプがより使い易いものとなって IT 社会の中で普及し、社会に広く貢献していくものと期待される。

３．タイムビジネスに関する海外の状況

３．１　調査の概要

３．１．１　調査目的

タイムビジネスの研究開発、実用、普及を促進していく観点からも、海外におけるタイムビジネスの最新状況を把握し、それを踏まえて活動を促進する必要があり、海外調査を実施した。

本調査は、タイムビジネスに関連する欧州各国の制度及びサービス状況に関する総合的な調査・分析を行い、今後のタイムビジネスに関する推進に資することを目的とする。

３．１．２　調査項目

・タイムビジネスに関連する欧州各国の制度に関する調査
　時刻配信やタイムスタンプといったタイムビジネスに関する事柄が、電子署名や電子取引に関係する法律や規制でどう扱われるかについて調査する。
・タイムビジネスに関連する欧州各国のサービス状況に関する調査
　時刻配信やタイムスタンプといったサービスが、国または私企業でどのように提供されているか、また、どのように利用されているかについて調査・分析する。
・タイムビジネスに関連するベンダの実績に関する調査
　必要な機器を提供するベンダの情報により、実際に時刻配信やタイムスタンプのサービスがどのような組織あるいは私企業で、どのようなサービスに利用されているかを調査・分析する。

３．２　タイムビジネスに関連する欧州の制度

ヨーロッパにおいてタイムスタンプの利用に影響を与えた法規には、以下が挙げられる。

- 電子署名指令（Digital Signature Directive）- EU
- インボイス指令（Invoice Directive）- EU
- BaselⅡ Financial Regulations（グローバル）
- サーベンス・オクスリー法（Sarbanes-Oxley Act）- アメリカ
- 刑事証拠法（Criminal Evidence Act）- イギリス

当初、本報告ではタイムスタンプに関する法規の中で、EU 電子署名指令での取り扱いについて、特に以下の点について述べる予定であった。

- 電子署名指令におけるタイムスタンプの位置付け
- EU 構成国が各国において電子署名指令を導入した際の、国による相違点（タイムスタンプに関して）

しかし、ヨーロッパにおけるタイムスタンプの利用に関しては、先に挙げた他の法規についても電子署名指令と同程度の影響を与えたと思われることから、併せて取り上げることとする。

３．２．１　EU 電子署名指令におけるタイムスタンプの位置付け

（1）　序章

電子署名指令の採択と施行

電子署名指令は 1999 年 12 月に採択され、EU 構成国は 2001 年 7 月までに、各国において必要な法令を定めることが求められた。

目　的

電子署名と特定の証明書サービスについて、法律上の枠組みを確立すること。

適　用

証明書サービスプロバイダ（CSP: Certificate Service Provider）、署名作成装置を認定する団体、および電子署名を利用する団体。

電子署名指令では、電子署名を行うにあたってタイムスタンプの使用を義務付けていない。また、様々な種類の電子署名（第 5 条 1 項、第 5 条 2 項）について規定しているものの、タイムスタンプについては直接言及していない。

（2） タイムスタンプと電子署名指令

タイムスタンプは、電子署名指令において証明書サービスの一部と考えられている。電子署名指令の説明部[9]では、証明書サービスについて以下のように定義している。

証明書サービスは、証明書の発行と管理に限られるべきではなく、電子署名を利用する、または電子署名に付随するあらゆるサービスを内包するべきである。こうしたサービスには登録サービス、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、または電子署名に関連するコンサルティングサービスなどが含まれる。

このように、タイムスタンプサービスは“電子署名に係わる問題や、電子署名の利用をサポートするサービスのひとつ”であると定義している。しかしこれは、タイムスタンプサービスプロバイダがタイムスタンプサービスの提供にあたって、電子署名指令による規制を受けると示唆するものではない。指令が重きを置いているのはタイムスタンプサービスを提供するサービスプロバイダではなく、あくまで適格証明書（qualified certificate）を提供するサービスプロバイダである。

つまり、電子署名指令の付属書Ⅱ（適格証明書を提供するサービスプロバイダに関する規定）に定められた要件は、適格証明書を公共的に提供するサービスプロバイダに対して適用されるものであって、タイムスタンプを提供するサービスプロバイダに対しては適用されないことになる。

３．２．２ タイムスタンプの管轄機関

2000 年以降の電子署名指令の導入・実施にあたり、EC はヨーロッパの標準化団体である CEN/ISSS（Committee for Standardization/Information Society Standardization System）と ETSI（European Telecommunications Standards Institute）に対して、電子署名利用の普及促進に伴う新たな標準化活動の必要性について、調査するよう命じた。これによって、European ICT Standardization Board の後援のもと、European Electronic Signature Standardization Initiative（EESSI）が開始された。

このイニシアチブでは、電子署名に係わる将来的な標準化要件についての報告書が作成された。この報告書では、電子署名の証拠能力（署名が為されてから長期間経過した後も、その真正性を持続・証明する）の確保にあたって、保存（アーカイブ）サービスが重要な役割を果たすとしている。また、こうしたサービスについての標準が存在しないことから、保存サービスを更なる調査を必要とする分野として特定している。

この報告書は、ETSI によるタイムスタンプに係わる様々な標準の開発につながった。

3.2.4 節に後述するように、他の法規においても、電子文書の保存におけるタイムサービスの利用が注目を集めており、EESSI 報告書は非常にタイムリーなものであったと言える。

３．２．３　EU 構成国における相違点

タイムスタンプの利用は、オーストリア、ドイツ、イタリア、ポーランドにおける電子署名法令では明確に述べられており、タイムスタンプの法的定義が定められている。これらの定義は、大体においてタイムスタンプが“証明書サービスプロバイダによって発行・書名された証明書で、プロバイダが特定のデータが特定の日時に提示されたものである事を認定するもの”と定めている。また、タイムスタンプは主に「あるデータが（タイムスタンプが為される以前に）存在し、タイムスタンプが為されて以後改ざんされていない」ことを証明する手段として利用されている。

いくつかの国においては、タイムスタンプサービスプロバイダが認定機関からサービスの認定を受けることもできる（任意）。こうした国々にはオーストリア、ドイツ、ルクセンブルグ、イギリス、ポーランドが含まれる。

ポーランド

ポーランドにおいてタイムスタンプは“データに付随する電子フォームで、電子署名や電子認証を受けたデータと論理的な関連性を持っており、日時の特定および電子署名の検証のためにサービスプロバイダによって生成されたデータ”であると規定される。

上述の例外国を除き、殆どの構成国では大きな修正を加えずに、電子署名指令を自国の法令に取り入れている。また、修正が加えられた場合でも、それらの変更点はタイムスタンプに全く影響がないものとなっている。

EU が製作した電子署名指令の導入・実施ガイドラインでは、各構成国における必要な法令の整備にあたって、タイムスタンプに関する規定を含めることは特に指示していない。しかしタイムスタンプに関する規定を取り入れたことによって、ドイツのようにタイムスタンプの産業界への普及を促進した国もいくつかあると考えられる。

３．２．４　タイムスタンプと他の法規定

本章のはじめに述べたように、EU の電子署名指令の他にも、ヨーロッパにおいて電子署名とタイムスタンプの利用に影響を及ぼした法規がいくつか存在する。

- インボイス指令（Invoice Directive）- EU
- 電子調達指令（E-Procurement Directive）- EU
- BaselⅡ Financial Regulations - グローバル
- サーベンス・オクスリー法（Sarbanes-Oxley Act）- アメリカ
- 刑事証拠法（Criminal Evidence Act）- イギリス

どの法規においてもタイムスタンプが直接に言及されているわけではない。しかし、どの法規も文書の保存に関する要件を定めている。中には電子媒体での保存を認めているものもあり、それに伴い保存文書の改ざん防止が要件となっている。

（１）　インボイス指令（Invoice Directive – EU）

インボイス指令は 2002 年の 1 月に採択され、全構成国において 2004 年 1 月までに各国の法令に取り入れるよう求められた。この指令の主要目的は、企業の発行するインボイス（送り状/請求書）に記載されるべき項目を規定することである。これには売上税徴収の観点から、構成国における税金情報を一定の形式に統一し、スムーズな取引を促進するという意図があった。この他にも、インボイス指令は 2 つの重要な問題について提議している。

- インボイスはある程度の期間について、保存されなければならない（ベルギーの例では 10 年間）
- インボイスを電子的に発行・保存してもよい

インボイス指令では、インボイスの真正性とデータの完全性が保証された場合、構成国が電子インボイスを受容しなければならない旨を定めている。指令では前述の要件を満たす実装手段として、先進電子署名（advanced electronic signature）と、EDI（Electronic Data Exchange）の 2 つの方式を認めている。また、構成国では任意で適格電子署名の利用を要求することができる（例：ドイツ）。しかし、指令ではインボイスへの電子署名を法的意義から要求しているのではないことを明確に述べており、先進電子署名と適格電子署名をあくまで技術的意義に基づくものとしている。尚、構成国は自国の裁量において、自由に他のタイプの電子インボイスを採用することが認められている。

インボイス指令ではタイムスタンプの利用は義務付けられていない。しかし、インボイスが電子的に保存されるのであれば、いかなる改ざんも不可能とするような方法で保存し

なければならないとしている。実際には、そうした保存は電子署名とタイムスタンプの併用によってのみ可能となる。ドイツはインボイス指令を同指令の制定と同年度に、他国に先駆けて導入した。また、ドイツにおけるインボイス指令の実装は、全ての電子インボイスについて適格証明書の利用を要求するなど、最も厳格なものとなっている（日付の保存に伴い、タイムスタンプも要件とされる）。

他国においては、インボイス指令をおおよそデフォルトに沿った形で導入している。以下にベルギーの事例を取り上げる。

ベルギーとインボイス指令

ベルギーではインボイス指令をむしろ一語一句に近い形で自国の法令に取り入れた。ベルギーの VAT 規則（Code de la TVA：付加価値税に関する規則）ではインボイスの真正性とデータの完全性が保証されていることを条件に、電子インボイスを原則的に認めている。また、指令に指示されているように、先進電子署名と EDI を共に電子インボイスの実装方式として認めている。他のタイプの電子インボイスについては、真正性と完全性に関する一定の条件が満たされれば、大蔵大臣による認可がおりることもあり得る。こうした電子インボイスは、そのインボイスの発行に利用された実装方式が正式に認可されている国においてのみ、その法的有効性が認められる。

インボイス指令 2001/115 では、構成国自身でインボイスの保存期間と、（ある程度において）保存場所を定めることを認めている。構成国ではインボイスをオリジナルのまま保存するよう定めることもできる。しかし、どのような場合においても、インボイスの真正性、完全性、可読性が保存期間を通じて保証されなければならないという点は共通要件となっている。保存に使用するメディアやフォーマットなど、他の点においては強制していない。

ベルギーの VAT 規則では、インボイスは紙・電子媒体に係わらず、オリジナルのまま 10 年間保存されなければならないと定めており、同時にインボイスの真正性、内容（データ）の完全性、可読性が保存期間を通して保証されなければならないとしている。また、真正性や完全性を保証するためのデータ（公開鍵証明書など）においても、同様に保管されなければならないと規定している。

ベルギーの徴税機関では、電子インボイスの管理方法を明確にする文書の整備を進めている。そのための技術的なワークグループも設立され、メンバーには企業（Isabel、Certipost、Ubizen）、ICODIF[1]、行政機関が加わっている。こうした動きの中で、タイムスタンプは

[1] Institut de Codification des Distributeurs et des Fabricants/Instituut voor de Kodering van de Distributeurs en de Fabrikanten – ベルギー・ルクセンブルグにおける EAN（European Article Number）団体

VAT 規則に基づいて電子インボイスを作成、交換、保存するのに適していると考えられている。

インボイス指令では電子インボイスのセキュリティに関して、ある一定のセキュリティレベルを満たすように指示するのではなく、構成国が必要に応じて異なるレベルのセキュリティを要求することを認めている。従って、電子インボイスのセキュリティ要件に関する各国の法令は多様化している。具体的には、インボイスの完全性の保証のみを要求するものから（スウェーデン、フィンランド）、適格電子署名の利用を要求するものまで（ドイツ、スロバキア、スペイン）、多岐にわたっている。インボイス指令は電子インボイスサービスの出現にも一役を果たしており、主に銀行とビジネスクライアントとの間で利用されている。例としては Deutsche Bank と BNP Paribas がこうしたサービスを提供しており、技術基盤として PKI（公開鍵基盤）とタイムスタンプを利用している。

（2） 電子調達指令（e-Procurement Directive – EU）

EU 電子調達指令は、EU 構成国が物資・サービスの調達にあたってインターネットベースのシステムを開発することを奨励（強制）する目的で採択された。この指令は、インターネット上での入札告知から実際の入札まで、全てのプロセスを電子化するというビジョンを掲げている。タイムスタンプは全プロセスにおいて要求されるが、とりわけ入札において重要となる（入札や申込みが “ いつ ” 行われたのかを確認）。

電子調達指令は、EU の内部市場戦略（Internal Market Strategy）の一部である。EU 構成国では、2006 年までに物資の公共調達の大部分を電子化することが目標とされ、リスボン戦略と並行して 2010 年までに電子公共調達を広範囲にわたって普及させることを目指している。

（3） 刑事証拠法（Criminal Evidence Act – イギリス）

イギリスではセキュリティ対策として、ビデオカメラが公共の場や私有のビルにおいて幅広く設置されている。こうしたビデオカメラによる映像は、時おり裁判における証拠物件として提示される。この種の証拠物件の信用性は、ある程度において映像が撮られた日時に依存する。こうした監視カメラを運用する会社では、タイムスタンプを採用することによって、映像が証拠として受け入れられる可能性を高めることができると考えている。こうした背景から、監視カメラの分野におけるタイムスタンプの利用が拡大している。

（4） その他の法規定

国際的な銀行業務規約は、BaselⅡ Financial Regulations によって厳格化された。この法規では様々な規定に加えて、広範囲に及ぶ文書の保存が義務付けられている。サーベンス・オクスリー法は、Enron の会計スキャンダルの後に制定され、アメリカ企業、また、アメリカにおいて事業を営む外国企業に、BaselⅡ同様、広範囲に及ぶ文書の保存を義務付けている。

こうした文書の維持・保存が要求されたことにより、企業では紙ベースや、マイクロフィルムベースのシステムに比べてより費用対効果の高いソリューションとして、文書の電子保存を真剣に検討し始めている。

３．３　タイムビジネスに関連する欧州のサービス状況

本節では、欧州におけるタイムスタンプサービスの発展について、以下の観点から述べる。

- 政府系機関
- 民間産業
- タイムスタンプの産業別の普及
- タイムスタンプを利用した、最も一般的なアプリケーションの概要（提供ベンダと、利用している産業セクタ）

本文に先立って、AuthentiDate 社の最高経営責任者（CEO）である Wedenburg 氏の、タイムスタンプと電子署名の利用に関するコメントを以下に記す（AuthentiDate はビジネスプロセスにおける電子データの検証サービスを提供する米国企業)。

一般的に、認証サービスは次の 3 つの項目を取り扱う：

- Who（誰が）
- What（何を）
- When（いつ）

“ 誰が ” と “ 何を ” は通常取引処理（トランザクション）に係わってくる。この場合、電子署名が利用されるが、タイムスタンプの利用は不可欠ではない。一方、“ 何を ” と “ いつ ” は通常文書（電子的に保存する文書、または電子インボイス）に係わってくる。この場合タイムスタンプが重要になる。つまり、タイムスタンプは “ 人 ” や “ 取引 ” にはあまり必要とされていないが、“ 文書 ” や “ 文書の処理プロセス ” において、よく利用されていると考えられる。

３．３．１　政府系機関とタイムスタンプ

（1）　概評

電子署名指令と EU 競争法（Competition Law）は、政府の PKI システムに関する制限を設けている。例えば、政府は電子政府サービス用の電子署名をサポートするための PKI システムを構築することはできるが、公共セクタの外部に及ぶ PKI システムを構築することは認められていない。

表 3.1 に、様々なヨーロッパ諸国において、電子政府サービスにアクセスするのに必要とされるデジタル証明書のタイプを示す。なお、表中の略語については下記の通りとする。

- SSCD: Secure Signature Creation Device（セキュアな署名生成装置）
- QC: Qualified Certificate（適格証明書）
- CSP: Certificate Service Provider（証明書サービスプロバイダ）

表 ３．１　電子政府サービスへのアクセスに要求される証明書の種類

国名	証明書	SSCD	法的根拠
アイルランド	QC 以外の証明書	要	第 5 条 2 項
イギリス	認定 CSP 発行の QC	不要	第 5 条 2 項
イタリア	認定 CSP 発行の QC	要	第 5 条 1 項
エストニア	認定 CSP 発行の QC	要	第 5 条 1 項
オーストリア	QC 以外の証明書	要	第 5 条 2 項
オランダ	認定 CSP 発行の QC	要	第 5 条 1 項
スウェーデン	QC 以外の証明書	不要	適応法令 第 5 条 2 項
スロヴェニア	QC	要	第 5 条 1 項
チェコ共和国	認定 CSP 発行の QC	要	第 5 条 1 項
デンマーク	QC 以外の証明書	不要	適応法令 第 5 条 2 項
ドイツ	認定 CSP 発行の QC	要	第 5 条 1 項
フィンランド	QC	要	第 5 条 1 項
ベルギー	QC	要	第 5 条 1 項
ポーランド	QC 以外の証明書	不要	特別法令
ルーマニア	QC	要	第 5 条 1 項

表 3.1 より、エストニア、スロヴェニア、チェコといった新規加盟国で、適格証明書の利用が採択されていることがわかる。この理由は、ひとつには、適格証明書以外に基づくデジタル署名（第 5 条 2 項に規定）よりも高度なセキュリティが必要であるというこれらの国々における認識であり、もうひとつには、ドイツの近隣諸国への影響力の結果であると思われる。これらの国では、自国の企業がドイツとビジネスを行うにあたり、同様の法令や規制を採択した方が何事にも容易であると見ている。こうした事情から、バルト 3 国、ポーランド、チェコ共和国は電子署名指令・インボイス指令共にドイツに類似した形で導入している。

電子調達指令については、ほぼ全 EU 構成国において適格証明書を採用している。これは電子調達というプロセスには他のタイプの証明書では不適切であるという見方によるものと考えられる。オーストリアの事例を挙げると、情報サービスへのアクセスには他のタ

イプの証明書の利用を認めているものの、電子調達システムの開発に参加するためには、適格証明書が唯一認められた証明書となっている。

標準規格

EU 構成国はデジタル署名システムの導入にあたって、ETSI 標準 TS 101 903（XAdES）を採用している。この標準はタイムスタンプについても取り上げている。従って EU 構成国の政府による（デジタル署名を利用した）システムであれば、タイムスタンプについても付随的にカバーしていることになる。

イギリス

イギリスでは、大手通信事業者である BT（British Telecom）を含む多数の企業が、電子政府サービスにアクセスするためのデジタル証明書を発行している。これらの企業はどれも政府とは無関係の組織である。こうしたことから、イギリス政府では電子政府サービスにアクセスするための市民や企業に直接係わる活動の多くをアウトソーシングしていると言える。同様のことはタイムスタンプサービスにも言える。政府がタイムスタンプサービスを提供することもあり得るが、これは政府内でのセキュアな通信の確保のためなど、厳密に政府内専用のサービスとなる公算が大きいと思われる。

ドイツ

ドイツは電子署名指令の国内法への導入にあたり、タイムスタンプについても進んで取り入れた。インボイス指令の導入時についても同様である。そうした国内法は、ドイツ産業界におけるデジタル署名とタイムスタンプの利用を奨励したものと考えられていた。しかし 2004 年 10 月にドイツの経営コンサルティング会社である Mummert Consulting により公表された報告書「電子政府における電子署名（“ Electronic signatures in e-government “ ）」によれば、ドイツの地方自治体における電子署名の導入率は非常に低いままであり、真の電子政府の実現を遠いものにしている。

同調査によれば、電子署名を利用しているのは地方自治体の僅か 8%である。更に、市民も企業も、電子政府サービスの提供が限られていることもあって電子署名を積極的に利用しているとは言い難い。調査では、市民と企業への電子署名の普及率の低さ、また（電子署名を利用する）電子政府サービスの提供が限られていることが重なって、電子政府への誘発剤となるはずの電子署名の普及が行き詰まっていると指摘している。

ドイツ市民は平均して年 2 回、公文書のやり取りを行うという。電子署名を利用するには約 30 ユーロの費用が掛かるため、単純に割るとすれば、一般的な市民であれば申込み初年度において一文書（取引）の単価が 15 ユーロという計算となる。地方自治体も含め、この費用の高さが電子署名の普及の障害となっているという見解があり、前述の調査によれば 75%の地方自治体がデジタル署名を市民に無料で提供するべきであると考えている。

今後数年の間に、大規模な連邦政府プロジェクトがドイツにおける電子署名の普及を促進する可能性もある。そうしたプロジェクトには 2006 年に導入が開始される健康保険カード（Health Insurance Card）、2007 年に開始される求職者向けの求職カード（Job Card）、将来的な電子 ID カードなどがある。また、電子調達システムの導入も電子署名（およびタイムスタンプ）の利用を促すものと思われる。

エストニア

エストニア政府は、国民に対してマイクロチップを搭載した PKI ベースの ID カードを発行している。このプロジェクトには 2 つの側面がある。ひとつは国民にセキュアな身分証明証を提供することであり、もうひとつは ID カードを利用してアクセスする電子政府サービスを提供することである。EU への加盟に伴い、エストニア政府には近隣諸国とのビジネスがシンプルかつ容易に行われることを確実にしたいという切実な想いがある。このため、エストニア政府は電子政府における ID カードの利用について、フィンランドと MOU（Memorandum of Understanding）を締結した。MOU の目的のひとつは、エストニアとフィンランド両国において電子文書が法的に同等であることを確約することであった。サービスの提供にあたっては、エストニア政府自身では電子署名サービスもタイムスタンプサービスも提供していない。代わりに 2 つの銀行と 2 つの通信事業者から成るグループが行っており、このグループによって、AS Sertifitseerimiskeskus（SK）と、タイムスタンプサービスの提供および ID カードの発行・利用基盤となる認証局（CA）が設立・運営されている。グループの目的のひとつは、以下の要件を満たす電子署名文書を発行することである。

- 法的に完全に有効であること
- 任意の目的に利用できること
- 長期間にわたって有効性を備えていること（タイムスタンプとの併用により実現）
- 国際標準・EU 指令に準ずること

また、エストニア電子署名法（2000）では、以下の要件を規定している。

- EU 電子署名指令の規定に準ずる先進電子署名の利用のみ認可する
- 適格証明書の利用を要求する
- 電子署名に対し、手書き署名と同等の効力を制約なしに付与する
- 認証局（CA）とタイムスタンプ局（TSA）に関する監査規定を設ける

従ってエストニア政府では、CA/TSA を兼ねた民間企業を利用して、政府主導の PKI システムを構築していると言える。

スペイン

スペインでは、PKI 技術を用いてユーザ認証、データの完全性、秘密性および利用足跡をトレースするサービスを提供する Safelayer 社が、法務省に興味深いアプリケーションを提供している。このアプリケーションはスマートカードを利用して文書へのアクセス制御を行うもので、タイムスタンプを使用して、「いつ」「誰が」「どの文書に」アクセスしたか追跡することを可能にしている。

（2） 欧州電子化計画 （eEurope）

2002 年に、EU は eEurope 2002（欧州電子化計画）を始動させた。このイニシアチブには多くの目的がある。

第 1 段階：情報提供（Information）- 公共サービスに関する情報をオンラインで提供
第 2 段階：一方向交流（Interaction）- フォームのダウンロード
第 3 段階：相互交流（Two-Way Interaction）- フォームの処理、認証
第 4 段階：取引の確立（Transaction）- 個別ケースへの対応、決定、デリバリー（支払い）

EC が実施した調査によれば、第 1 段階と第 2 段階の導入については、殆どの EU 構成国において完了している。しかし、文書の電子保存に伴い PKI とタイムスタンプが要件となる第 3 段階と第 4 段階については進展しておらず、いくつかの構成国においては少しずつ導入されているが、他の構成国では未だ実施されていない状態となっている。

こうした第 3 段階・第 4 段階にあたるサービスの導入の停滞に対して、EU は eEurope 2005 を始動させており、いくつかの推薦事項を示している。

- 顧客指向のポータル・ソリューションを通じて、調整の取れたサービス供給に注力する
- バックオフィスの再編成とプロセスの統合を通じて、管理手順の簡素化に注力する
- セキュアな基盤の構築に注力する

バックオフィスの再編成とプロセスの統合には、データの電子的な保存とタイムスタンプが必要になるため多くの政府にとって難題となっており、こうした課題への取り組みはまだ始まったばかりである。同時に、様々な企業が電子政府アプリケーションやサービスを将来有望な市場として認識し始めている。3.3 節に、そうした企業の事例を取り上げる。

（３） 電子調達（e-Procurement）

EU 構成国政府では、電子調達をコストの削減と競争力の改善・向上に役立つ分野として考えている。EU の電子調達指令は、構成国に対して電子調達ポータルの導入を急ぐよう説いている。電子調達プロセスでは、タイムスタンプの利用が文書の提出（入札告知が有効な期間内に提出されているか）と、文書の保存（将来照会が必要となった時に安全・確実に保存してあるか）の両方に必要となる。殆どの政府では、電子調達システムに参加を希望する企業のために、PKI と適格証明書の導入を進めているが、ヨーロッパにおける電子調達はまだ初期段階に留まっている。オーストリアの事例を挙げると、同国は電子調達の導入にいち早く着手したものの、まだ表 3.2 に示すような状況となっている。

表３．２　オーストリアにおける電子調達制度の導入状況

プロセス例	達成度
入札公告にかかわる通知	やや進捗
入札公告の公表	やや進捗
入札公告の提出・受領の管理	低
入札公告の検証	低
発注	低
インボイス（請求）	低

上記から、オーストリアではある程度タイムスタンプを利用しているが、限られた範囲であることが察せられる。また、多くの場合において、PKI サービスを提供しているのは政府自身ではなく、外部団体となっている。一方、電子調達の分野において主導的立場に立っているドイツの状況を下記に示す（表 3.3)。尚、このデータは、2004 年に公表された EU 報告書「構成国政府における電子調達制度 E-Procurement Member State Governments」」からのものである。

表３．３　ドイツにおける電子調達制度の導入状況

プロセス例	達成度
入札告知にかかわる通知	高
入札告知の公表	高
入札告知の提出・受領の管理	高
入札告知の検証	自動化には至っていないが、２年以内に自動化される予定
発注	高
インボイス（請求）	高

また、デンマークも電子調達おいては抜きん出ている。表 3.4 は電子調達の分野での、デンマークの主要組織についてまとめている。多くは非政府系団体か、政府のコントロール下にはないと見なされる団体である。これらの団体は、デジタル証明書の発行とタイムスタンプの実施を、電子調達プロセスの一部として行っている。デンマークにおける電子調達に係わる活動は、以下の調査結果からも広範囲にわたっていることがわかる。

- 国家機関の 54%が、電子調達システムを利用している
- 地方機関の 63%が、電子調達システムを利用している
- ローカル機関の 34%が、電子調達システムを利用している

[出典：”IT ipraksis®2003”, RAMBOLL Management]

更に、公共調達ポータル（DOIP：Danish Public Procurement Portal）における 2003 年度の取引高は約 500 万ユーロとなっており、著しい増加傾向を示している。

表３．４　デンマークの電子調達制度に携わる組織

電子調達システム	主要組織
公共調達ポータル（Public Procurement Portals）	www.doip.dk – 2002 年に開始され、Gaterade 社によって運営。ポータルはウェブベースのシステムであり、Oracle Exchange Software を基盤としている。現行バージョンでは電子オークション、電子カタログ、バックオフィス・システムとの統合をサポートしている
	www.rakat.dk – 民間企業である COMCARE 社によって運営。主要用途は電子購入（注文と電子インボイス）であり、地方・ローカル併せて 40 団体によって導入されている
	www.kmd.dk – 民間企業である KMD Webindkob 社によって運営。主要用途は電子購入（注文と電子インボイス）であり、地方・ローカル併せて 70 団体によって導入されている
	http://ski.ethics.dk, www.netkatalog, www.netindkob – National Procurement Ltd.によって運営。主要用途は電子入札告知
電子署名（Electronic Signature）	www.digitalsignature.dk – 導入されているが、電子公共調達には利用されていない
電子カタログ（Electronic Catalogues）	利用あり
電子オークション（Electronic Auctions）	多少利用あり
ダイナミック購入システム（Dynamic Purchasing System）	利用なし
フレームワーク協定（Framework Agreements）	国家レベル、地方レベル、ローカルレベルの行政機関によって利用

下記の表 3.5 に、デンマークにおける電子調達システムの状況についてまとめる。

表３．５　デンマークにおける電子調達制度の導入状況

プロセス例	達成度
入札告知にかかわる通知	高
入札告知の公表	やや進捗 - 今後 3 年間での成長が見込まれる
入札告知の提出・受領の管理	低 - 今後 3 年間での成長が見込まれる
入札告知の検証	低 - 今後 3 年間での成長が見込まれる
発注	やや進捗 - 今後 3 年間での成長が見込まれる
インボイス（請求）	低 - 今後 3 年間での成長が見込まれる

スウェーデンは、電子調達の導入に関してデンマークと類似した段階にある。デンマーク同様、スウェーデンにおいても電子調達に係わる大多数のサービスが民間企業によって提供されている。他の主要構成国（フランスやイタリアなど）は、まだこれからと言った状況となっている。こうした状況から推測されるように、これらの今後取り組み予定の国々におけるタイムスタンプの利用度は低くなっている。

新規加盟国と電子調達

EU 新規加盟国[2]においても電子調達の導入が進められているが、非常に基本的なレベルからの取り組みとなっている。殆どの新規加盟国では、第 1 段階「情報のオンラインでの提供」を進めているが、これらの国々も今後 3 年の間に第 4 段階まで導入が進むことが見込まれる。なお、新規加盟国の中では、現時点でスロヴェニアが最も進んでいると思われる。

[2] チェコ、エストニア、キプロス、ラトビア、リトアニア、ハンガリー、マルタ、ポーランド、スロヴェニア、スロヴァキア

タイムスタンプ・プロジェクト

ヨーロッパでは、重要な機能としてタイムスタンプに係わるプロジェクトが数多く実施されている。表 3.6 にプロジェクトの事例を挙げる。

表３．６　ヨーロッパのタイムスタンプ関連プロジェクト

プロジェクト	概要
ArchiSig[3]	ドイツ出資のプロジェクトで、電子署名とタイムスタンプを利用した長期的な電子文書の保存に係わる取り組み（終了済）
OpenEvidence	2002 年に開始された 5th Framework Programme のプロジェクト。データの保存のための、データ認証とタイムスタンプに関するフレームワークの開発（終了済）
Timesec	ベルギーのプロジェクトで、タイムスタンプとセキュリティに係わる基本要素の利用に係わる取り組み
Erpanet	6th Framework Programme のプロジェクト。文化遺産と科学をデジタル媒体として保存するための、実現可能で明確な情報、ベストプラクティス、および技術の開発に関わる取り組み

[3] http://www.sit.fraunhofer.de/cms/de/forschungbereiche/tad/prjekte_/ArchiSig.htm

３．３．２　民間産業とタイムスタンプ

ヨーロッパには、数多くの非政府系タイムスタンプサービスプロバイダが存在する。多くのタイムスタンププロバイダは、通常幅広い PKI サービスの一環としてタイムスタンプサービスを提供している。表 3.7 にヨーロッパにおいてタイムスタンプサービスを提供している民間企業の例を挙げる。また、可能な限り当該企業がサービスの提供（普及）に注力している地理的要件を示すものとする。

表３．７　ヨーロッパ民間企業によるタイムスタンプサービス

提供ベンダ	サービス提供地域	概要
AuthentiDate（ドイツ）	ドイツ、ベネルクス（ベルギー・オランダ・ルクセンブルグ）、オーストリア	アメリカを本拠とする企業だが、ドイツに強い。他ベンダと提携している
Zertificon（ドイツ）	ドイツ	タイムスタンプを利用した電子メールアプリケーションに重点を置いた PKI システムを提供
Utimaco（ドイツ）	ドイツ	SAP に準拠した、幅広いセキュリティ関連サービスを提供
Guardeonic（ドイツ）	ドイツ、イギリス、ベネルクス（ベルギー・オランダ・ルクセンブルグ）	Infineon の子会社。幅広いセキュリティ関連サービスを提供
Unizeto（ポーランド）	ポーランド	ポーランド国内においてサービスを提供
Cryptotech（ポーランド）	ポーランド	暗号化技術とスマートカードシステムに注力。銀行を中心に 20 社以上の顧客を持つ
nCipher（イギリス）	ヨーロッパ	ハードウェアベースの TS サービスを提供。幅広い企業を顧客に持つ
Security & Standards（イギリス）	イギリス	イギリスを本拠とする SI。様々なセキュリティ製品を提供（www.secstan.co.uk）
Ascertia（イギリス）	イギリス	イギリスを本拠とする SI。電子インボイス、文書の電子保存にはあまり係わっていない
Edelweb（フランス）	フランス	主に大企業に対して、タイムスタンプサービスを含む、幅広いセキュリティサービスを提供。文書の電子保存に携わっている

提供ベンダ	サービス提供地域	概要
Kotio （フランス）	フランス	フランスのサービス産業にセキュリティサービス（主に TS・PKI）のアウトソーシングを提供
Posteasy （フランス）	フランス	セキュアな電子メールサービスと電子インボイスサービスを提供。幅広い中小企業および法人団体を顧客に持つ
Akhela （イタリア）	イタリア	セキュリティに重点を置いた SI サービスを提供
C & A （イタリア）	イタリア	SI。主にイタリア国内において、TS・PKI サービスを提供
Cybernetica （エストニア）	エストニア	研究開発機関。EU による資金援助を受けており、現在のところ無料の TS を提供している（近いうちに変更予定）。”Truesign” DS/TS システムを開発
Privador （エストニア）	エストニア	Truesign システムを提供する SI
Netlock （ハンガリー）	ハンガリー	企業および個人ユーザ向けにサービスを提供
Trustport （チェコ）	チェコ	幅広いセキュリティサービスを提供
PVT Prokom （チェコ）	チェコ	チェコのトップ SI 企業。幅広いセキュリティ関連サービスを提供しており、特に文書の電子保存に強い
Xicrypt （オーストリア）	オーストリア	タイムスタンプサービスや、ハードウェアベースのセキュア電子メールと電子インボイスサービスを提供
Safelayer （スペイン）	スペイン、ポルトガル	典型的な PKI を利用した、エンドユーザとの間の取引処理（トランザクション）とアクセス制御を提供。主に政府機関と銀行を顧客とする
Interactiva （スペイン）	スペイン	セキュリティベンダ。セキュリティコンサルティングと電子インボイスサービスを提供する

３．３．３　タイムスタンプの産業別の普及

イギリスのセキュリティサービスベンダである nCipher 社では、ヨーロッパにおいてデジタル署名を利用している企業は何千社とあるが、タイムスタンプをそれなりに利用しているのは多くとも数百社であると見ているという。この見解は、PKI の発展状況から推察すると、妥当なものであると思われる。PKI の導入が大企業では進むものの、中小企業では未だ検討中であるのと同様に、タイムスタンプは殆どの企業にとってまだ見極めの段階にあると思われる。こうした傾向はヨーロッパ全体において見られると考えられる。なお、中にはタイムスタンプに関して、他国よりも積極的な取り組みが取られていると思われる国もある。

- ドイツ - 法規の後押しを受け、様々な TS アプリケーションが提供されている
- イタリア - 法規の後押しを受け、様々な TS アプリケーションが提供されている
- フランス - 法規の後押しを受け、電子インボイスに係わる TS アプリケーションが提供されている

また、PKI やタイムスタンプは、利用するか、利用しないか、ユーザに依存する傾向が強いとも考えられる。ドイツの PKI システムベンダである Zertificon 社はセキュアな電子メールサービス（PKI（S/MIME）をサポートし、タイムスタンプサービスも具備）を提供している。Zertificon は幅広いドイツ企業を顧客に持っており、その多くはサービス産業であり、また、いくつか政府系機関（地方警察や地方行政機関など）も含まれる。サービス産業は主に銀行と金融機関が占めており、宝くじの運営企業や製造業者などもいくつか含まれている。

3.3.4 節に後述するように、タイムスタンプは、電子インボイスや文書の電子保存といったアプリケーションにおける機能的要素のひとつである。電子インボイスは企業に対してコスト削減の上で高い優位性を提供する。しかし、電子インボイスはようやく一般に受け入れられ始めたところであり、既に電子インボイスシステムを利用している Dow Chemical 社のような企業はかなりの早期導入者であると言える。従って「特に電子署名・タイムスタンプの利用が進んでいる」と判断できる産業セクタはまだ存在しない。

こうした状況下において、ドイツで最近実施された法改正の影響によって健康保険会社が文書の電子保存の利用に関して主導的な立場を築きつつある。保険会社は膨大な量の書類を取り扱っているが、法改正によってこれらの書類を電子的に保存することが認められることとなった。大多数の企業が、大規模なコストの削減につながると見ており、文書の電子保存への移行に積極的に取り組んでいる。

他国においては、特にタイムスタンプが必要とされるアプリケーションの導入を積極的に進めている産業セクタは見受けられない。nCipher によれば、イギリスにおいていくつかの大規模な公立図書館が文書の電子保存を検討しているという情報もあるが、具体的なレベルには至っていないと推測される。表 3.8 に実際にタイムスタンプサービスを購入している企業（nCipher 社顧客）を挙げる。

表３．８　nCipher のクライアント企業と業界の分布

金融機関		
BACS	Bank of America	Barclays Bank
Cheshire Building Society	CitiGroup	Deutsche Bank
Egg	EQ Online	Ergo
Fleet Bank	MasterCard International	NTT Data
認証局 CA		
eCertify	GlobalSign	GTE
Identrus	Interclear	Mixrosoft
Netscape/AOL	PrincewaterhouseCoopers	VeriSign
ISP/ASP		
XO Communications	MSN Hotmail	Exostar
通信事業者・ワイヤレス事業者・移動通信事業者		
Commerce	AT6T	GTE
Lucent	Smart trust	Verizon
その他の業種		
GigaTrust	E.ON Energie	Exostar
iPIN	Petsmart.com	Royal Mail
UK Department of Work and Pensions		Sporting Index
U.S. Department of Defense	Securify	

nCipher 社の顧客企業の産業別分布によれば、金融業界が最もサービスを利用している産業セクタであるとも見えるが、その他の業界についてもそれほどの差異なく重要な顧客ベースであると考えられる。こうした状況や、本節 3.3 のはじめに示した Wedenburg 氏（AuthentiDates 社）のコメントを踏まえると、今後タイムスタンプの導入が見込まれるビジネスセクタとしては以下が考えられる。

- 膨大な量のインボイスを取り扱うビジネス
- 相当量の書類（紙ベース）の保管が要求されるビジネス

３．３．４　最も一般的なタイムスタンプサービスの概要

（1）　アプリケーション

デジタル署名とタイムスタンプを組み合わせて利用する代表的なコアアプリケーションは、以下の 2 つである。

- 電子インボイス（ビジネスプロセス）
- 電子保存（文書・データ）

その他にも、デジタル署名とタイムスタンプを利用した、これらのコアアプリケーションに派生するサービスが幅広く存在している。ここでは事例としてイギリスの SI である Security and Standards と、フランスの SI である Kotio のサービスを取り上げる。

Security and Standards では、同社の“ GT Evidence Manager ”システムの中で、デジタル署名とタイムスタンプサービスを提供している。同システムにおいて提供されている製品は以下の通りである。

- GT Evidence Manager – 証拠の真正性管理と封印(evidential seals)を行う、冗長性を備えたサーバ。
- GT Evidence Toolkit – 希望のアプリケーションに証拠サービスを統合するための、ソフトウェアツール。
- GT Evidence Mail and Mailroom – 送受信に係わらず、電子メールや添付ファイルに封印（evidential seals）を施すアドオン・サービス。電子メール基盤に追加。
- GT Evidence Office – ファイル内容の封印（evidential seals）を行うアドオン・サービス。文書エディタ、オフィスアプリケーションに追加。
- GT Evidence Voice & Video – マルチメディア情報（ボイスメール、ビデオ会議など）に封印（evidential seals）を施すサービス。
- GT Evidence Universal File Sealer – あらゆるタイプのファイルに封印（evidential seals）を施すデスクトップ・アプリケーション。
- GT Evidence Witness – ウェブページに封印（evidential seals）を施す、ブラウザへのアドオン・サービス。

一方、Kotio でも、企業の既存の IT 基盤に統合できる同様のサービスを提供している。

- E-Mail – 送受信に係わらず、電子メールを検査し、タイムスタンプを施して、セキュアな場所に保管する。

- Time Stamper – 電子ファイルに、電子署名およびタイムスタンプを施す。
- Web Signing – オンライン取引に、電子署名およびタイムスタンプを施す。
- Digital Archive – 電子ファイルをセキュアな外部施設に保管する。タイムスタンプを施すことによって“いつ”保管されたかを記録する。
- E-Business – グループ内において署名・検証プロセスを通じて文書の共有を可能にする。B2B 取引を可能にする。

AuthentiDate によると、多くの企業は機能完備・統合済のマルチ機能システムを購入するという（例えば、電子インボイスを利用するのであれば、文書の電子保存も併せて購入）。また、AuthentiDate では、どのサービスを購入する場合でも、電子メールに対するタイムスタンプと認証サービスは自動的にバンドル化する傾向が見られるという。

このように、多くの企業では、タイムスタンプをデジタル署名と組み合わせて提供している。中にはタイムスタンプとデジタル署名技術のみを提供し、個々のビジネスニーズに合わせたシステムへの統合は顧客自身に任せているベンダもあれば、AuthentiDate のように、システムインテグレーションまで行っているベンダもある。

表 3.9 に示すのは、AuthentiDate の顧客の概要である。デジタル署名やタイムスタンプの普及に関して他の国々がドイツより遅れていることを考慮に入れると、ドイツでの企業の導入例は、他の国でも受け入れられそうなタイムスタンプ関連サービスの傾向を示してくれることも期待された。

しかしながら、表からわかるように、タイムスタンプの利用に関して特出した傾向は見られないことがわかる。製造業よりも、サービス産業においての方が普及しているようにも思えるが、製造業大手の Dow Chemical が既に導入していることもあり、今後製造業界においてサービス導入の牽引力となることも考えられる。

表３．９　AuthentiDate のクライアント企業と提供サービスの概要

顧客	サービス概要
T-Systems （ドイツ）	他企業に対する、タイムスタンプとデジタル署名を利用した電子インボイスサービスの提供。サービスは Deutsche Bank の子会社である T-Telesec を介して提供される
T-Mobile （ドイツ）	電子インボイスを受け付けている顧客との間での電子インボイスサービス（タイムスタンプを利用）を提供
IS KV （ドイツ）	健康保険会社 300 社に対してソフトウェアと SI サービスを提供。これはドイツ国内市場の 30%にあたり、1900 万件の保険契約に相当する
KKH （ドイツ）	大手健康保険会社。タイムスタンプサービスを文書処理（保険金請求・インボイス）と保存に利用。システムは KKH のスキャンサービスプロバイダである Cocq Datendienst によって導入された
German Ministry of Economics & Labor	送受信文書へのタイムスタンプを含む、文書管理システムでの使用
National Car Rental （ドイツ）	ドイツ国内の拠点において、AuthentiDate の e-Billing Signature Solution を導入。適格電子署名を利用した電子請求書を採用した初めてのレンタカー会社でもある
Claimsoft AG （ドイツ）	紙ベースの書類管理対策として、建設業界で使用されているソフトウェアにタイムスタンプシステムを統合
SER Solution （ドイツ）	同社の DOXiS Enterprise Content Management Suite に、AuthentiDate の署名技術を統合
Esker Software GmbH （ドイツ）	SAP ユーザ向けの e-Billing ソリューション。2002 年 1 月からドイツの税法では、適格電子署名を利用したものに限り、電子請求書の受領者は税前減額の対象となることを保証している
DICOM （イギリス）	DICOM のデータキャプチャシステムと Authentidate のタイムスタンプシステムを統合
Dow Chemical （ヨーロッパ）	2001 年の電子請求書の利用に関する指令を含む、様々な EU 指令に準拠するため、AuthentiDate の e-Billing Signature Solution を導入。インボイスに係わる費用を 90%削減

セキュア電子メールとタイムスタンプ

セキュア電子メールは、タイムスタンプの活用が期待されるアプリケーションである。先に挙げたように、いくつかのベンダではタイムスタンプを電子メールサービスへのアドオンアプリケーションとして提供している。しかし、ドイツのセキュリティベンダである Guardeonic 社では、セキュア電子メールが幅広くは受け入れられていないと見ており、理由として以下を挙げている。

- ユーザへの要求が多い（証明書の管理と検証は常に問題となる）
- コストが高い
  - 証明書の管理
  - アプリケーションのインストール
  - ユーザ・トレーニング
  - ウィルス対策ソフトウェアのインストール
  - 一元的なコンテンツ・フィルタリングの欠如
- セキュリティポリシーによる制御の不能

こうした問題に対して、次善的なソリューションは存在している。例えば、全ユーザが個別ソリューションを必要とすることはまずない。その場合、そうしたユーザに対しては一元的にサーバで管理するソリューションを採用することによって、ユーザの負担や管理・検証の手間を軽減できると予想される。

オーストリア：Xicrypt

オーストリアのセキュリティベンダである Xicrypt は、様々なオーストリア政府機関（社会保障、財務、産業系）に対して電子インボイスソリューションを提供している。また、同社ではブリュッセルに本拠を置くヨーロッパの標準化団体である CEN（Committee for Standardization）にワークフローシステムの提供を行っている。

イタリア：Infocamere

Infocamere は、イタリアの商工会議所（Chambers of Commerce）に対して IT サービスを提供している。これらのサービスはセキュア電子メールと文書の電子保存に利用される電子署名とタイムスタンプを含む、幅広いものとなっている。

（2） タイムスタンプを提供している企業

タイムスタンプサービスや、タイムスタンプが重要な要素となるサービスを提供しているベンダの多くは、そのビジネス範囲が当該企業の本拠地（国）に制限されている傾向があるように思われる。3.3.2 節においてタイムスタンプサービスを提供している企業を挙げたが、nCipher の事例を除き、サービス提供区域が地域的に集中していることがわかる。

例えば、AuthentiDate は主にドイツ語圏の国々（ドイツ、オーストリア、スイスの一部）に対して同社の製品およびシステムインテグレーションサービスを提供している。他ベンダにおいてもサービスの提供に際して、言語的、もしくは地理的な要件が共通項となっていることがわかる。

これは、タイムスタンプサービスを提供するプロバイダが、ある特定の産業セクタを対象としてマーケティングを行っているのではなく、むしろ、電子インボイスや文章の電子保存などに興味を示しそうなあらゆる企業を対象としてマーケティングを行っているものと考えられる。こうした事情から、とりわけタイムスタンプを活用していると断定できる産業セクタを抽出することが困難になったと思われる。

タイムスタンプサービスは、単純に電子メールにタイムスタンプを施すだけのものから、電子インボイスや文書の電子保存を含む一連のビジネスプロセスまで、非常に幅広いアプリケーションに利用されている。そうした観点から見ると、タイムスタンプの機能性が複雑なものであることがわかる。本節ではこうしたタイムスタンプ関連サービスを提供している企業の概要を後述する。また、併せてヨーロッパにおけるタイムスタンプ関連サービスの第一人者である企業の見解（インタビュー）について記すものとする。

EU 内の地域差

ヨーロッパにおいて、ドイツがタイムスタンプ関連サービスのリーダー的存在であると見られていることは先に述べた通りである。しかし、他国の企業でも EU 指令に基づきビジネスチャンスを開発する利点を認識し始めていると思われる。フランスの大手銀行である BNP Paribas では、2003 年に Kotio のシステムを導入して、企業向けの電子インボイスサービスの提供を開始している。また、同時期にフィンランドの Nordea Bank も同様のサービスを始めている。

フランスでは様々な企業が電子インボイスサービスを提供している。これはフランスが EU 電子署名指令の採用にそれほど熱心でなかったことを考慮すると些か興味深い。しかし、フランスは基盤となる PKI が普及しており、幅広く利用されている。このことが電子署名・タイムスタンプという PKI 要素を利用する電子インボイスサービスの普及を促進したとも考えられる。フランスにおいて電子インボイスサービスを提供している企業には、Asterion、B-Process、Deskom、Posteasy、SwiftMail、Trust&Pay などがある。これらの企業全てが税務当局に認定された電子インボイスをサポートしているわけではない。しかし、全てのシステムにおいて文書の電子保存はサポートされており、タイムスタンプ機能が実装されている。

SAP と電子インボイス

世界有数のソフトウェアベンダである SAP は、企業のインボイス費用を大幅に削減するシステムとして、同社の SAP Biller Direct と SAP Billing Consolidation を電子インボイスソリューションとして提供している。企業の電子インボイスの導入を奨励するため、SAP では様々な調査を引用してマーケティングを行っている。例えば、市場調査およびコンサルティング会社であるアメリカの Celent Communication 社では、電子インボイスが紙ベースのインボイスと比較して 1 枚 4.80 ユーロのコスト削減につながると見積もっており（2001 年）、同じくアメリカの調査会社である Gartner 社では 3 ドルの削減と試算している（2003 年）。SAP では、月に約 7 万 5 千枚のインボイスを処理する典型的な中規模企業では年間 270 万ユーロのコスト削減を実現できると指摘している。これらの調査ではインボイスの受領者側においても、最高 50%のコスト削減が見込まれるとしている。

提携

3.3.2 節に取り上げた企業の多くは他の企業と提携している。これらの企業は相互にサービスやシステムを提携し合うことにより、全体として完全なシステムの提供を可能にしている。例えば nCipher は、タイムスタンプサービスのサブシステムを AuthentiDate に供給している。このような提携内容は“up-stream パートナーシップ”と見なされる。“down-stream パートナーシップ”は、次に述べる AuthentiDate とドイツの Oce 社のような提携内容を示す。

Oce 社はドイツに本拠を置く企業であり、主要事業はコピー機製造業であるが、写真複写とストレージビジネスへと方向転換しつつある。Oce ではサービスの一環として、AuthentiDate のデジタル署名とタイムスタンプシステムを同社の製品に統合した。これによって Oce は保険会社などの顧客に対して幅広い文書保存サービスを提供することを得た。現時点では顧客の殆どがドイツ企業となっている。しかし、同社が国際的な企業であることを考えると、今後ヨーロッパ全域にサービスの提供を拡大していくものと見込まれる。

ドイツ：Guardeonic

Guardeonic 社は現在ヨーロッパで台頭しつつある典型的なセキュリティシステムインテグレータであり、幅広い分野を手掛けている。Guardeonic は IC 製造業者である Infineon の子会社であり、大多数の EU 構成国をサービス対象としている。商業活動においては、政府系機関、ヘルスケア、産業、金融の 4 分野に注力している。

ここで、ヘルスケアと金融がいわゆる“産業”から別枠で認識されているのは興味深いと思われる。タイムスタンプサービスを提供する他の企業においても、こうした区分け傾向が見られる。これは、タイムスタンプサービスの早期導入者であるヘルスケア産業および金融業界と、導入には慎重であるが大規模な市場である産業および政府という構図を反映したものと考えられる。

政府系機関に対して、Guardeonic では以下の製品/サービスを提供している。

- Portal Security
- Mobile Security
- Identity and Access Management
- Secure Process Integration
- Web Service Security
- Data Security
- Secure Communication
- Biometrics

タイムスタンプサービスは主に文書の取り扱い等にかかわる“ Secure Process Integration ”の分野で利用されるものと見込まれている。他のサービスの多くは成熟期にあって拡張を続ける PKI アプリケーションであるアクセス制限やスマートカードに関連したものになっている。Guadeonic の設立初期からの顧客にはドイツ政府がおり、税金関連申請書と売上税申告書のオンラインフォームについて、電子保存サービスを提供している。下記に Guadeonic システムにおけるタイムスタンプの位置付けを、同社の Secure Work Flow System に示す（図 3.1）。

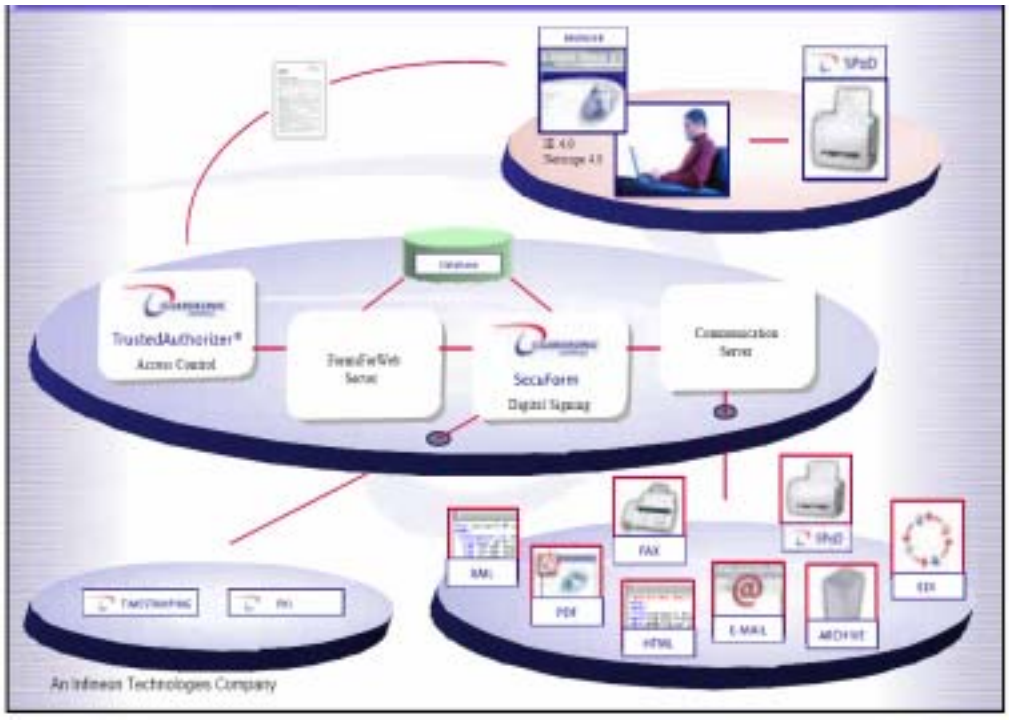


図３．１　Guardeonic Secure Work Flow System **概略**

Guardeonic では、政府官公庁におけるバックオフィスの再編成が、ようやくヨーロッパ各国で始まったと見ている。この結果、統合化が進むに伴い、ユーザがより多くの情報に簡単にアクセスすることが理論上可能になる。こうしたシステムの実現には、同時にセキュリティと管理機能の強化が要求されることになる。こうした高度なセキュリティと制御機能の提供は、PKI によって実装できると考えられている。

フィンランド：Nordea

Nordea はフィンランドの銀行であり、スカンジナビア諸国、ドイツ、ポーランドに支店を持つ。同行は e-Banking の分野において技術的リーダーであると見なされている。表 3.10 に Nordea の提供する e-Banking サービスと、顧客による利用率を示す。

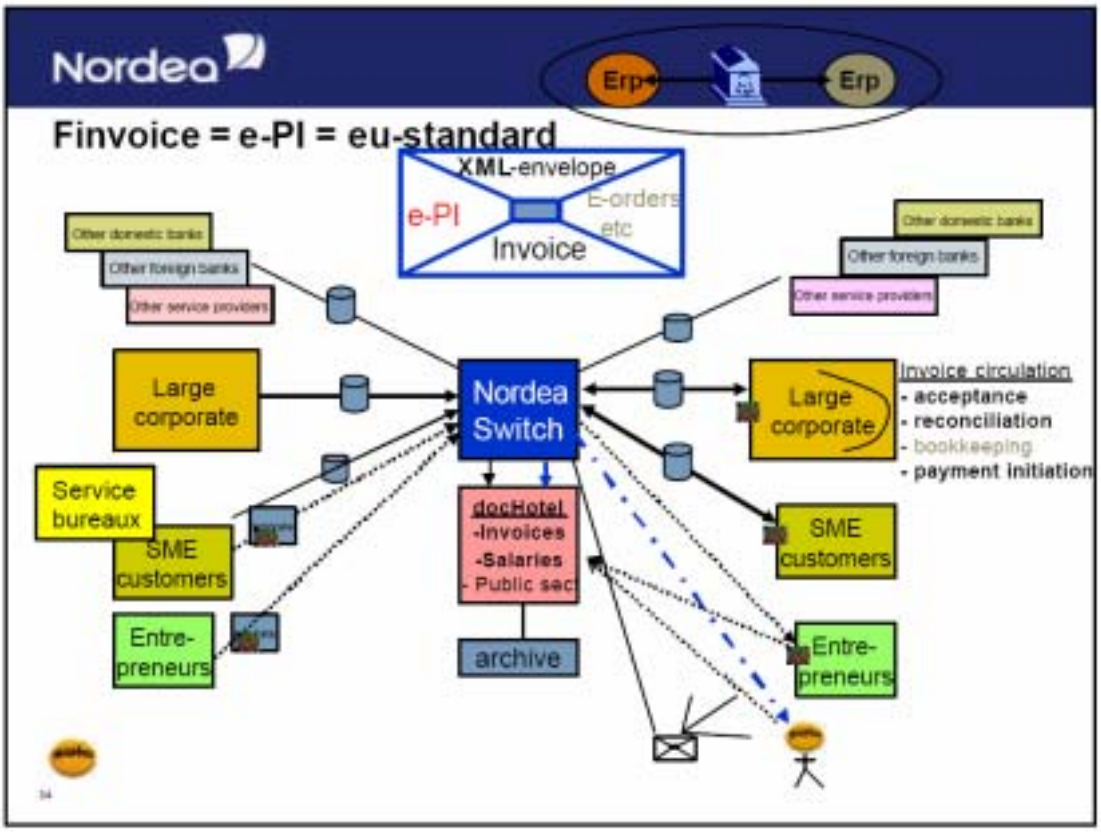
表３．１０　Nordea Bank の e-Banking サービス

サービス	利用率
普通株の買い注文	80%
学生ローン（書類不要）- DA	73%
投資信託	60%
個人/小額の海外送金	63% （大企業ではほぼ 100%）
一般顧客向けオンライン決済	49%
消費者ローン（書類不要）- DA	31%
自動車ローン - DA	28%
住宅ローン（ローンについては書類不要、但し不動産譲渡証書については書類要）	20%
外貨交換	19%

“DA（Digital Archival）”によって示したサービスにおいては、電子フォームの保存機能が要求されるため、タイムスタンプが必要となる。現在 Nordea では企業顧客をターゲットに、コストの削減を誘引力として電子インボイス（B2B）ソリューションの導入提案を進めている。また同行では B2C における e-Billing サービスについても提供している。これらのサービスは、政府系機関と政府系機関に納入しているサプライヤーへの拡張も進んでいる。

Nordea が提供する電子化ソリューションで、電子保存（タイムスタンプ）の導入を推進するもうひとつのサービスは e-Salary である。このアプリケーションでは、従業員に対して給与支払通知を電子的に提示することによって、紙媒体の給与明細の供給を省略することが可能になる。

図 3.2 は、Nordea がサービスの提供を見込む顧客ベースと、こうしたシステムをサポートするのに必要とされる基盤を示している。文書の電子保存機能が必要とされることから、タイムスタンプサービスの実装も自動的に付随要件となっている。



[出典：http://europa.eu.int/comm/enterprise/ict/policy/legal/dublin/naatsaari.pdf]

図３．２　Nordea Bank のサービス基盤概略

（3）タイムスタンプを提供している企業の見解

Unizeto（ポーランド）：最高技術責任者（CTO） Wilenski 氏

Unizeto はデジタル証明書と様々なタイプのタイムスタンプサービスを提供しており、銀行、研究開発機関、行政機関、保険会社、企業など幅広い分野の企業によって利用されているという。

Wilenski 氏の見解では、電子署名指令を国内法に取り入れた際にタイムスタンプについても取り扱ったことも手伝い、ポーランド国内におけるタイムスタンプサービスは順調な滑り出しを遂げたと見ている。

タイムスタンプと電子署名の結合はその重要性が一段と増しており、また、文書の電子保存が真に機能するためにも、タイムスタンプサービスは不可欠となっている。Wilenski 氏によれば、中期的には電子保存がタイムスタンプを推進する主要なアプリケーションになるという。また、ポーランド政府がドイツ政府の例に倣って、電子インボイスについてもドイツと同様の法令の制定を検討していることから、これが実現すれば、タイムスタンプサービス市場の発展に拍車がかかるものと見ている。

ポーランドにおけるタイムスタンプ市場の実際の規模は Unizeto においても正確に把握していないようである。業種的には現在銀行と金融の利用が多くなっているが、書類の多さに悩まされている企業であれば、どこも潜在的な顧客ベースと見ているという。

最後に、ポーランド政府では電子政府サービスに対する取り組みにも力を注いでいるという。こうした取り組みの中でも電子署名といったサービスには注目が高まっており、利用の促進につながっていると見られている。

PVT Prokom（チェコ共和国）

PVT Prokom は幅広いセキュリティ関連サービスを提供している。これらのサービスには文書の電子保存も含まれており、PVT Prokom では 14 社を顧客例として挙げている。Bosch の事例を除き、殆どの顧客が政府もしくは政府系機関となっている。12 の企業のうち、3 社（Central Securities Register、Energy Regulator、Czech National Health Insurance）において、タイムスタンプサービスが必要となっている。東欧においてもタイムスタンプサービスは存在するが、これはドイツなどと比較すると低いレベルから始められている。また、文書の電子保存を利用している企業のタイプはドイツのそれと類似しており、主にサービス産業の企業となっているが、チェコ共和国では健康保険会社もそうした企業として挙げられる。

AuthentiDate（ドイツ）：最高経営責任者（CEO）Wedenburg 氏、マーケティング責任者（Marketing Director）Balfanz 氏

AuthentiDate は米国企業であり、様々なタイムスタンプソフトウェアアプリケーションを開発している。同社はドイツ支社を通じて、ヨーロッパでも強力な存在感を示している。AuthentiDate では、ソフトウェアとシステムのセールスに主に 2 通りの方法を取っている。

- エンドユーザへの直接販売
- OEM や SI を通した間接販売

AuthentiDate は以下の企業と提供しており、これらの企業では多くの場合、主に AuthentiDate の製品を自社製品にバンドル化している。

- DICOM（イギリスに本拠を置くが、ヨーロッパとアメリカもカバーしている）
- Oce（ドイツのコピー機製造業者）
- Unicomputer（ドイツのシステムインテグレータ）
- Mikromatic（ドイツの文書管理サービスプロバイダ）
- Filenet
- GFT Hyperarchiv
- Saperion

Balfanze 氏によれば、タイムスタンプ市場を強力に促進した重要な法規が 2 つあるという。ひとつは電子インボイスの認可性について取り扱ったもので、もうひとつは売上税に関するものである。

Wedenburg 氏は、インボイス指令を電子インボイスサービスの導入に拍車をかける重要な推進力になると見ているという。彼によれば、ドイツ国内において電子インボイスを採用している企業では、適格電子署名とタイムスタンプを利用している。また、電子インボイスは企業にとって大規模なコスト削減につながると指摘しており、ドイツの旅行会社である Schmetterling 社は電子インボイスに対する投資を 2 ヶ月以内で回収し終え、Dow Chemical においてはインボイスの発行費用を 90%削減したと述べている。

AuthentiDate はビジネスの焦点をドイツに合わせているが、インボイスとデータの電子保存サービスを他の市場においても提供している。National Car Rental はイギリスのレンタカー会社であり、AuthentiDate のシステムを利用して、ヨーロッパでインボイスサービスを提供している。Wedenburg 氏によれば、ヨーロッパではヨーロッパ規模の電子インボイスシステムの開発をドイツの法規に準じて行う傾向があるという。この背景には、インボイス指令をより厳しく導入したドイツの国内法に準拠したシステムであれば、ヨーロッパ中どこにおいても受け入れられるという通念がある。Dow Chemicals が AuthentiDate をベンダに選んだのにはこういった理由もある。

電子署名・タイムスタンプの普及

Wedenburg 氏は、競合相手が少ない現状において、AuthentiDate は電子署名・タイムスタンプにおいてリーダーであると考えている。大企業はコストの削減につながる文書の電子保存に非常に高い関心を寄せている。しかし同氏は電子署名・タイムスタンプサービスともに市場の活性化にはつながっていないと見ている。

nCipher（イギリス）：プロダクトマネージャ（Product Manager） Lewis 氏

グローバルレベルにおいて、Lewis 氏は、例えばアメリカなどと比較すると、ヨーロッパは電子署名とタイムスタンプの分野において、世界で最も進んでいると信じているという。また、同氏は日本においてはこれらの分野が産業主導で進められており、将来に向けて日本の取り組みが大きな発展を遂げることに期待している。

Lewis 氏は電子インボイスを電子文書保存といったより大きな市場の一部と見ており、このサービスがタイムスタンプサービス普及の主要なアプリケーションになると考えている。同氏は、電子署名には寿命があると指摘し、タイムスタンプと組み合わせることによって、長期間にわたって保全性の提供が可能となると述べている。

nCipher はイギリス国内において、紙ベースの書類の保存を課題としている大規模な公立図書館の相談を受けているという。これらの図書館では電子署名とタイムスタンプを利用した、改ざん防止機能を備えた電子保存形態に移行したいと考えているようである。

その他の分野におけるタイムスタンプの利用には、刑事事件の証拠として用いられるビデオカメラがある。イギリスの刑事証拠法ではタイムスタンプの利用を義務付けてはいない。しかし仮にタイムスタンプがあった場合には、裁判における証拠能力の認定がもっと容易になるだろうと指摘している。

企業に関して言えば、Lewis 氏は様々な法規と、文書の電子保存化に伴うコストの削減が電子署名とタイムスタンプの推進力になると考えている。同時に、これらの技術に何ができるのかといったユーザ教育の必要性を指摘している。

Lewis 氏はフランスとスペインが電子署名指令において柔らかなアプローチで臨んだと考えており、ドイツに見られたような推進が行われなかったと見ている。同様のことはタイムスタンプにも言えると考えられる。

Lewis 氏は、現在数千社がデジタル署名を利用しており、数百社がタイムスタンプを利用していると見積もっている。nCipher では、タイムスタンプ市場に今後も拡張の余地があり、また、市場がコストを抑えつつ法規に準拠していく必要性に後押しされているとの見解を示している。

３．４　ベンダの海外実績ヒアリング調査

時刻配信およびタイムスタンプのシステムに関する装置を提供するベンダで、海外において実績のあるベンダのヒアリングを実施し、どのような国の、どのような組織あるいは企業で、どのように利用されているかを調査した。

ヒアリング内容のまとめを表 3.11 に示す。

表３．１１　ベンダ海外実績まとめ

地域	国	組織・サービス	説明
北米	USA	US Postal Service- Electronic Postmark - AuthentiDate	米国郵便 USPS の電子郵便の内容証明サービス
		Arab Labs, US - Electronic Post Mark	インターネット郵便での証明サービス
		WetStone Technology Inc, US - TA and TSA, Digital Evidence	時刻配信・タイムスタンプ事業
西欧	UK	Security and Standards, UK - digital evidence	E-Commerce における取引に関して電子証明を与えるサービス
		Lloyds of London - Kinnect	ロンドンの保険市場およびロイズにおける Kinnect（保険引受けプラットフォームシステム）での信頼性・セキュリティを高めるための電子証明 http://www.kinnect.com/
		BT Ignite, UK - legal document transfer	ブリティッシュテレコムの EC サービスで、契約等の文書へのタイムスタンプサービス
		British Library - document archival	英国図書館での文書アーカイブ（紙をスキャンした電子データ）用途のタイムスタンプ
	フランス	Kotio - Trust Services - Paris	フランスのセキュリティ関連会社 KOTIO が企業の重要な電子メールに日時証明を行うサービス
	ドイツ	PTB Germany - Time Authority	ドイツ計測研究所が時刻配信をサービス
	ベルギー	Belgacom- CertiPost and eID project	ベルギー通信会社の電子郵便サービスおよび電子署名サービスにタイムスタンプを適用 http://www.belgacom.be
東欧	ハンガリー	Matav - Hungarian telco : trust services	ハンガリーの電話会社がサービスしている電子署名サービスの一環としてタイムスタンプサービスを実施
		Hungarian Tax Authority - on-line tax payments	ハンガリー税務局が税金のオンライン申告に対してタイムスタンプを付与

地域	国	組織・サービス	説明
東欧	ポーランド	Centrast - Polish Government CA	ポーランドの政府 CA のサービスで時刻配信
	チェコ	PVT AS - Trust Services Czech Rep	タイムスタンプを含むサービスを提供
		Komercni Banka, Czech Repblic - bank wide PKI	銀行内の PKI でのタイムスタンプサービス
	スロバキア	ViaSec - Slovakia	タイムスタンプを含むサービスを提供
南米	メキシコ	Secretary of the Economy Mexico - Government PKI	銀行内の機密文書への電子公証サービスにて、タイムスタンプを付与
		CENAM (National Metrology Institute) - Government TA	メキシコ政府の TA
	ブラジル	Observation Nacional Do Rio De Janeiro - Brizilian Time Keeper	ブラジルの国家計量機関（時刻機関）の TA、TSA サービス

３．５　海外状況のまとめ

米国企業改革法（Sarbanes-Oxley Act）や新 BIS 規制等では、規制準拠の証明のための各種電子書類の証拠性が問われ、電子署名とともにタイムスタンプの利用が促進されると推察される。

EU 電子署名指令おいては、タイムスタンプは、電子署名の機能を補完するものと理解されており、完全な電子署名を求める際に必要なものと認識されている。したがって法・規制において電子署名とタイムスタンプが一体化して扱われる傾向がある。EU 電子署名指令の導入・実施ガイドラインでは各構成国における法整備に関してタイムスタンプを含めることを直接には求めていないが、ドイツ、オーストリア、イタリア、ポーランドにおける電子署名法ではタイムスタンプの利用を明確に述べている。これらの国ではタイムスタンプの利用を規定に明確に取り込むことによって、タイムスタンプの実際の利用が普及促進されている。

また EU インボイス指令や EU 電子調達指令など、EU では具体的な請求や調達の業務に関して電子署名およびタイムスタンプによって証拠性を確保し、電子化を推進していくことが示されている。

海外でのサービスでは、米国におけるメールの内容証明サービスのように時刻および内容を証明するサービスが既に立ち上がっている。一方、ヨーロッパではドイツの署名法や EU 電子署名指令等でタイムスタンプの必要性が認識されていることもあり、電子署名等の幅広い PKI サービスの一環としてタイムスタンプを提供している例も多く、電子署名とタ

イムスタンプの双方を用いた実際のサービスを提供している例も多い。具体的には大量の請求処理を行う電子インボイス関連、文書・データの電子保存でのタイムスタンプの利用が多く見られる。

４．おわりに

平成 16 年度の調査研究分科会では、タイムビジネスに関する国内状況および動向を把握するために、各業界を代表する団体や組織と意見交換会を広く実施した。タイムスタンプの認識については業界によってばらつきがあったが、タイムスタンプの必要性を強く認識する業界団体もあり、意見交換や議論の内容は制度や技術についてレベルの高いことも多かった。それ程までに意識が高いとは予測しておらず、認識を新たにするなど、有意義な意見交換会が実施できたと考える。意見交換にご協力を頂いた各種業界団体や業界関連組織の方々に感謝の意を表したい。

海外調査については、制度面から実際のサービスまで、海外の状況を全体的に把握できた。平成 15 年度のドイツ視察の調査報告と合わせると海外の状況が広く把握でき、これまでに調査した海外の状況や動向は、今後の国内の発展に大変参考になるものと考える。海外実績のヒアリング調査に協力して頂いたベンダの方々に、心より感謝の意を表する。

なお、海外調査には韓国の視察調査を加える予定であった。しかしながら計画当時の諸事情に鑑みて延期せざるを得なかった。海外調査の残る課題として今後に期待したい。

本報告が今後のタイムビジネスの発展の一助となれば幸いである。

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
株式会社日立製作所
清松　哲郎

● 関連資料

● EU 電子署名指令

米丸恒治(訳)[4]

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ア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一

[4] 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。

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鍰項および付属書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[5]

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

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

---

[5] 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。

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.jp/time/