第４．２章

電子署名（ディジタル署名）法施行令理由書

署名法省令理由説明書

（1997年10月8日付連邦政府決定の案による）

A．一般的事項

省令はデジタル署名法についての必要な実施条項を含むが、イノベーティブな方式の余地を与えるため、含まれるのはデジタル署名法と同じく原則として目標設定のみであり、規定はデジタル署名法§1、1項の意味での安全な署名法を保証することに限定されている。署名法作成と検査にあたっての技術規格および実際のプロセスは省令の規律対象ではない。技術の詳細と実際のプロセスは§12、2項および§16、6項で予定されている所轄官庁の施行令で述べる。

B．個別事項

§1について（許可付与、撤回、取消しの手続）

1項について

文書形式は関係者の法的安全性に役立つことを目的とする。

2項について

申請者には2段によって、所轄官庁への必要な書類の提出を義務づける。それには例えば商業登記簿抜粋（商法§9、2および3項参照）が属する。このほか、所轄官庁は義務に従った自己の裁量で第三者からその他のインフォメーション、例えば申請者の納税義務履行とか流動資産についてのインフォメーションを取り寄せることができる（行政手続法§24参照）。個々の従業員の必要な専門知識は仕事の種類によって決まる。証明書発行機関はいずれにしても、デジタル署名法と署名省令の規定を満たすため法律・情報技術の専門知識が必要であり、それには厳しい基準を設けなければならない。

証明書発行機関が仕事の一部を第三者に委託する場合、その全体の責任は影響されない。証明書発行機関は仕事の一部を委託した第三者がデジタル署名法と署名省令から生じる義務をあますところなく果たすことを保証しなければならない。これが保証されない場合、許可が却下されるか、あるいは取り消されることがある。

証明書発行手続は証明書申請から、証明書のチェック可能状態保持、さらには§13の最終ドキュメント化までのすべてのプロセスを含む。

3項について

この規定により事情考量の原則が考慮される。行政手続法§28、2および3項とは異なり、組織上・技術上複雑な事情もあることを考え、誤った判断を避けるためにも、いずれにしても陳述聴取は行わなくてはならない。

§2について（費用）

1項では支払義務のある事項が定められている。1人の受益者に関わりのある主な事項はすべて含まれているが、個々の手数料はケースに応じて、実際にかかった時間をもとに、物件費も含まれる、2項の手数料レートから計算する。3項は正当性の理由による例外を規律したもので、その出発点となるのは許可付与のため計算された手数料である。そのほかの点では行政費用法が適用される。1件の許可のための手数料は最高3〜5千マルクと思われる。全体として、個別に計算できる作業に対しては完全な費用カバーが行われる。手数料レートは、挙げられた事項のコストカバー不足を避けるため、将来も所轄官庁によって定期的にチェックされる。

§3について（証明書発行の申請手続）

1項について

照合（1段）は証明書発行機関の受付事務所で行ってもよい。「その他適当な方法で」の照合には同等の安全性が必要である。

証明書への自署による申請（2段）は、1段の照合および§13、1項のドキュメント（提示された身分証明書のコピー）と並んで、（証明書発行機関の不正な従業員による、あるいは申請者の偽造身分証明書の提示による）証明書偽造の疑いが生じたとき、重要な証拠となる。照合の際、身分証明書と申請書の署名を確実に比較できるよう、申請書には受付事務所で署名することが必要である。

1人の人間に複数のサインコードに対し証明書を発行することができる。1つのサインコード証明書が付与されれば、その後の申請はデジタル署名法に従い、オンラインでサインコードにより行うことができる（3段）。詳細は証明書発行機関と申請者との契約合意に委ねる。

2項について

この項はデジタル署名法§5、2項に従い、申請者の希望により行われる、すでに存在する代行権あるいは許可の証明書への記載を規律するものである。ここでは2つの目標を設定する。まず第1に代行権または許可は確実に証明されなければならない。これには証明書発行機関による証明書とデータの専門上の検査が必要である。第2に代行権記載の際、第三者には証明書の内容およびそれを使用禁止とする可能性（デジタル署名法§8、2項）について教示しなければならない。

「第三者」には、自然人がその機関としてあるいはその代行者として行動する法人も含まれる。代行権を証明書に記入するとき、第三者が法人である場合、まず法人のため行動する自然人は代行権限（例えば業務管理者）を有しているか確認しなければならない。これは例えば、代行公正証書、あるいは商法§9による登記簿抜粋、あるいは代行権に関するデータを記載した付加証明書で行うことができる。「第三者」には、その代行権が証明書に記入された（自然または法）人のみ含まれ（デジタル署名法§7、2項）、その職業法上その他の許可に関するデータが記入された当の機関は含まれない。
許可に関するデータ（3段）を記入するには許可証の提示で十分であり、許可機関への教示義務はない。公法上の職業監督を行う機関（例えば医師会）は、職業上のデータを証明書に記入するための独自の証明書発行機関を設けるか、あるいは特定の証明書発行機関と協力契約を結び、その職業監督下にある人間はその機関でのみ証明書にデータを記入するよう指導することができる。コミュニケーションパートナーはこの機関の証明書を要求することができる（例えば認証の目的で署名法を使うとき）。
デジタル署名法§5、2項に記されているデータのほか契約ベースで他のデータをも証明書に記入することができる。

§4について（申請者への教示）
規定されている教示は、申請者をして将来のサインコード所持者として、安全な署名法を作成し、署名法を確実に検査し、権限のない者が彼のサインコードを悪用するのを防止し、間違ったデータにサインするのを防ぐため、彼自身必要な措置を講じることを可能ならしめることを目的とする。
教示された必要措置を行うのは申請者の責任であり、必要措置（例えば適切な技術コンポーネントの使用）を怠っても、その個人サインコードで作成された署名法の有効性には変わりない。

1項について
No. 1について
No. 1、3段の規定はサインコードの不正使用の追加保護が目的である。証明書発行機関が（例えばサインコードの付いたチップカードの）適切な破壊処分を引き受けることによりそれを行うこともできる。

No. 2について
No. 2に記されている、個人照合番号その他のデータ（例えばパスワード）漏洩の場合の変更は最新の方式では利用者自身も行うことができる。

No. 3 について
No. 3 に従い申請者には適切な技術コンポーネント使用の必要性とどの技術コンポーネントが法的要求を満たすかを教示すること。

No. 4 について
No. 4 の規定は、サインされたデータの受取人に、デジタル署名法§7、1 項 No. 7 のどの制限条項に注意すべきか、デジタル署名法§7、2 項のどの事項を守るべきかを直接知らせるのが目的である。

No. 5 について
サインされたデータの使用にとって日時が「重要」であるか否かは（No. 5）、個々の場合につき検討しなければならない。例えば新しい署名法では日付印が必要である（§18 参照）。

No. 6 について
No. 6 に関しては§18 およびその理由説明を参照。

No. 7 について
No. 7 による証明書有効性の確認は、証明書に対する署名法のチェックを含む。さらに証明書を証明書の公開リストでチェックするかは（そこに記載されているか、サイン作成の時点で有効かどうか）、サインを検査する者に任される。

2 項について
1 度教示を行えば、次回からの証明書申請では教示は行わなくてもよい。

§5 について（サインコードおよび照合データの作成とメモリー）
1 項について
この規定と§4 の教示とで高度の消費者保護が達成される。証明書発行機関は規定を満たすためサインコード所持者が例えば、安全性が§17 により検査され、確認されているチップカードを使用しているがどうか調べなければならない。そのため作成者はチップカードに認証手続を設けることができる。証明書発行機関が適切な方法で使った技術コンポーネントの安全性を確認できないとき、サインコード証明書の発行は見合わせなければならない。

2項について
この規定はコードあるいは照合データが証明書発行機関で漏洩したり、メモリーされたりするのを防ぐのが目的である。漏洩が完全には防げない場合、少なくとも発見できるようにする。証明書発行機関によってコード作成のため使われた技術コンポーネントはすでに§15の監察でチェックされる。そのほか、予定されているコードデータ媒体外での個人サインコードのメモリーはすでに技術コンポーネント（§16、1項参照）によって防止されている。
照合データに関しては（2段）、署名法をはじめて作成する前にサインコード所持者が新しい（自ら選んだ）データをインプットできるように、最新の技術コンポーネントを設定することができる。

§6について（サインコードと照合データの引渡し）
1段の規定は個人サインコードと照合データを確実に引き渡すのが目的である。引渡しの他の形式として、予定のサインコード所持者が希望し、それに伴うリスクをおかす気持があれば、例えば民事訴訟法によるサインコード所持者個人への正式の送達も考えられる。
サインコード所持者が、所持する証明書はデジタル署名法§4による証明書発行機関に由来するものかを必要があってチェックするには、所轄官庁の公開サインコード（2段）が必要である。サインコード所持者がそのコードを自ら作成し、証明書発行機関からは証明書のみ受け取る場合にも、公開サインコードを所轄官庁に引き渡すこと。

§7について（証明書の有効期間）
1段でサインコード証明書の有効期間が限定されているのは、署名法のための暗号方式が一定の期間についてのみ確実に評点が付けられるからである（§17、2項についての理由説明参照）。そのほかサインコード所持者にとって、証明書に記されているアルゴリズムとそれに属するパラメーターは証明書の有効期間中必要な適性を保持するとの確信が持てるものでなければならない。証明書上の署名法で§18の追加サインを避けるため（それに使ったアルゴリズムとパラメーターで証明書の有効期間が切れる前にもはや適性がなくなった場合）、証明書発行機関は証明書発行の際その安全性をも考慮しなければならない。

§8について（証明書の公開リスト）
1項について
挙げた期間内署名法はチェック可能でなければならない。
特に大量使用の際（例えば銀行やデパートで）署名法の検査をできるだけ簡略の行うため、証明書発行機関はその証明書リストの組合せによって、その都度重要な証明書はすべて（所轄官

庁の証明書も、また場合によっては外国の機関の証明書も）中央でチェック可能状態にしておかなくてはならない。度重なるオンラインでの問合せを避けるため、大量使用者には使用禁止リスト、および自動的に新しく使用禁止となった証明書を伝え、自己のコンピューターでのデータストックの訂正さえ行えばよいようにすることもできる。これに関する営業上のオッファは証明書発行機関に任す。
証明書発行機関は追加サービスとして、他のアルゴリズムあるいはパラメーターで作成された署名法のチェックをオッファすることができる。

2項について
証明書発行機関はそのサインコードを自ら作成し、所轄官庁がサインさえすればいいように証明書を完全に準備して、所轄官庁が証明書発行機関のため発行する証明書のフォーマットを自ら決めることができる（例えば自ら発行する証明書と同じフォーマット）。所轄官庁はそのサインの作成に際して証明書発行機関の希望により同じアルゴリズムとそれに属するパラメーターを使うようにすべきである。
証明書と技術コンポーネントでの統一規格の作成は担当の規格委員会と産業界の役目であるが、それには国際的な動向をも考慮すること。
デジタル署名法§15によりその署名法が承認される外国において複数の最高証明書発行機関が存在するとき（2段）、すべての最高証明書発行機関の証明書を受け入れること。この証明書発行機関は官庁により追加サインされるため（3段）、間接的にそこに由来する署名法のデジタル署名法§15による承認チェックはオンラインで行うことができる。
4段によって要求されている、公開サインコードの公示および所轄官庁証明書公開リストの電気通信番号の公示は、そこに記載されている証明書を認証チェックできるようにするのが目的である。

3項について
ここに挙げたケースでは証明書は、それが重要となるのは例外であるため（例えば§18により新しいサインにより「保存された」古いサインのチェックの際）、もはや常時呼出し可能な状態に保つ必要はない。個々のケースで問合せに回答するだけで十分である。しかしこれらの証明書を§13、2項による期限の切れたあとも、常時呼出し可能な状態にしておくのは少しも差し支えない。§13、2項についての理由説明も参照。

§9について（証明書使用禁止手続）
1項について

この規定はサインコード所持者、および代行権についてのデータが証明書に記された第三者の保護のためである。電話による連絡は実際上常時可能であるため、電話番号の公示によって即時使用禁止できるようにする。他の電気通信番号（例えばファックス）の公示は差し支えない。認証方法として例えばパスワード方式が考えられる。

2 項について
不正な使用禁止を防ぐため、使用禁止はここに挙げた前提でのみ可能とする。

3 項について
証明書がいつ禁止されたかについて疑問が生じないよう、使用禁止は最終的なものでなくてはならない。必要があれば新しい証明書を発行すること。サインコード所持者に対して使用禁止の確認を行うかどうかは契約合意に委ねる。遡及使用禁止はデジタル署名法§8、1 項 3 段により不可能である。

§10 について（従業員の信頼性）
証明書あるいは日付印の偽造ないし変造をできるだけ防ぐため、関係する者は信頼できる人間でなくてはならない。それには厳しい基準を設けること。特に、関連する犯罪（詐欺、横領、文書偽造）をおかした者は信頼できない人間である。

§11 について（技術コンポーネントの保護）
技術コンポーネントの不正使用に対する保護は技術上のマニピュレーションを防止するのが目的である。不正使用（物理的あるいは、例えば通信網を使って論理的に）は新たに使用される前に、少なくとも発見し、技術コンポーネントの交換あるいはチェックが行えるようにする。証明書もしくは日付印のサインに使われる、個人サインコードのついたデータ媒体は盗難に注意し、不正使用を防止しなければならない。

§12 について（安全計画）
1 項について
安全計画には証明書発行機関の安全措置の一覧を記すこと。プロセスオーガナイゼーションでは特に、 証明書もしくは日付印のサインに使われるサインコードをいかにして不正使用と盗難から守るかを説明しなければならない。また証明書のためのデータを偽造と変造から守る措置も重要であり、さらには証明書が当人の意向によりチェック可能な状態でのみ保持され、呼出し可能な状態では保持されないケースでは秘密保持のための措置も大きな意味を持ってい

る。このため例えば、証明書申請の受付事務所と中央機関の間のデータ（§3、1 項についての理由説明参照）をオンライン伝達の際サインし、暗号化することができる。中央機関によって発行された証明書は受付事務所が、証明書申請書のデータと一致するかをチェックすることができる。

証明書発行機関は少なくとも以下の技術コンポーネントを必要とする：サインコンポーネント（例えばチップカード）、証明書／日付印発行のための PC、§8 の証明書リストのためのサーバ。これに必要に応じて、サインコードと照合データ作成とチャージのための技術コンポーネントおよび日付印のための特殊サーバが加わる。§16 についての理由説明参照。

証明書発行機関の作業実施はさまざまな方法で（例えば提携契約によって）オーガナイズすることができるが、明朗経営で、義務サービスに対しデジタル署名法と署名省令の順守を保証することが必要である。全体の責任は個々の企業にある（§1、2 項についての理由説明も参照）。所轄官庁は場合によっては営業許可に義務を課することができる。

証明書発行機関が義務サービス（証明書と日付印発行）のほかに契約に基づき署名法に関連する他のサービスをオッファする場合は（例えば、他のアルゴリズムとパラメーターの付いた署名法のチェック）、それも安全計画に含ませなければならない。

安全計画は証明書発行機関特有の危険とリスクの説明をも含む。一般的な危険とリスクとはすでにデジタル署名法と署名省令の詳細な安全要求および§12、2 項および§16、6 項の措置施行令で考慮されている。

2 項について

措置施行令では、デジタル署名法と署名省令の規定を満たすための実際的な方法を例を挙げて説明する。これらの対策は範例的な性格を持つもので、他のイノベーティブな方法の余地を残すため、それと異なる方法も許容される。決定的な意味を持つのは、承認された専門機関によって法的整合性が確認されることである。直接的にせよ間接的にせよ、法的解釈は施行令の対象ではない。これは施行令の序文ないし導入部において適当な形で述べる。

所轄官庁（電気通信法§66 の規制官庁）はこの規定の宛先であり、施行令の記載と公表に責任を持っている。施行令作成に関しては署名省令は、規制官庁の全体にわたる権限にはかかわりなく、連邦情報安全技術局（BSI）の持つ専門権能を尊重する。BIS は BIS 設置法により情報技術システムの検査と評価ならびに情報技術安全の問題でのコンサルテーションを行う。BSI は行政手続法上の観点に立って職務共助に基づきそれを行うのではなく、施行令案を作成することにより BIS 設置法に従ったその責務の枠内で所轄官庁の作業を助けるのである。これはこの問題で連邦官庁組織において専門権能機関をさらに 1 つ余分に作るのを避けるのが目的である。取り入れらるべき安全措置に関し、できるだけ広範囲のコンセンサスを確保するため、作

成プロセスの各ステップで経済と学術の専門家の助言を求めること。責任規制官庁は、学界と経済界から提起された問題を解決に導き、決定を下す権限と義務を有する。

§13 について（ドキュメント）

1 項について

安全措置のドキュメント作成はデジタル署名法§13 および署名省令§15 による監察の実施のため必要である。その他の資料のドキュメント作成は、たとえば証明書偽造の疑いがあるとき必要である。それ以外に自動的にプロトコールデータ（例えば証明書発行機関の個人サインコード使用について）が作られるとき、そのドキュメントを作成するのは証明書発行機関の裁量に属する。

この最後の段の規定はドキュメント化されたデータが変造されないことを保証するのが目的であって、記録のサインには別のサインコードが必要である（デジタル署名法§4、5 項についての理由説明参照）。

2 項について

保存期間の計算は特に、民法§195 記載の規定の消滅時効期間（30 年）が重要でありうる署名法使用ケースでも、それに応じた保存期間が確保されるよう配慮したものである。この計算はまた証明書の許容有効期間をも考慮している。古い署名法が§18 に従い新しい署名法のよって長い期間「保存」される場合、消滅時効期間内では古い署名法チェックの可能性が保持できるようにする（例えば裁判所によって）。特定の分野（例えば医療）で、もっと長い保存期間が必要ならば、自己の証明書発行機関によってあるいは契約合意によってそれを確保しなければならない。

ドキュメント作成がデジタル形式で行われる場合（例えば証明書で）、「使える」とは「チェック可能」を含む。つまり、それに適したハード・ソフトウエアを備えなければならない。これに類した長い期間としては、例えば飛行機製造の「デジタルドキュメント」（50 年）、長期間にわたってデータを記入する電子土地台帳がある。

デジタル署名法§12、2 項の問合せ回答のドキュメントについては電気通信法§90 の場合と同じく 12 ヶ月の保存期間を定めている。

§14 について（営業停止）

1 項について

この規定は所轄官庁が 2〜4 項で義務づけされている、証明書発行機関営業停止の際の手続を監視できるようにするのが目的である。