第４章

電子署名（デジタル署名）法

第４．１章

電子署名施行令（Ｓｉｇ Ｖ）

署名法についての省令
（署名省令－SigV）
1997年10月8日付連邦政府決定の案による

1997年7月22日付デジタル署名法§16（連邦法官報Ⅰp．1870、1872）に基づき、連邦政府は以下の省令を公布する：

内容一覧

§1 許可付与、撤回、取消しの手続

(1) デジタル署名法§4、1項による証明書発行機関営業許可は所轄官庁に文書で申請のこと。

(2) 許可付与の前提を検査するため所轄官庁は必要な確認を行う。所轄官庁は申請者から必要な書類、特に証明書発行機関の法的代表者について、連邦中央登記法§30、5項により最新の商業登記簿抜粋、最新の品行証明書の提出を要求することができる。必要な専門知識証明のた

め申請者は、証明書発行あるいは日付印発行に従事する人間が必要な職業上の資格を有していることを説明しなければならない。

（3）許可の拒否・撤回または取消しを行う前に、所轄官庁は申請者の陳述を聴取し、彼に拒否・撤回または取消しの理由を除去する機会を与えなければならない。

§2 費用

(1) 以下の公的な仕事に対しては費用（手数料と経費）が徴収される：

1. 証明書発行機関営業許可
2. 許可申請拒否
3. 許可撤回あるいは取消し
4. 異議の完全または部分的却下
5. 証明書発行
6. §15、1項による検査報告と確認書のチェック
7. §15、2項による監査で、監査の際、デジタル署名法あるいは当省令に対する違反が無視できないものであることが認められた場合
8. デジタル署名法§11、2項によるドキュメントの引継ぎ

費用は、許可申請または異議の手続が開始されたが、その終了前に取り下げられた場合でも徴収される。

(2) 1項No. 1、5、6、7、8による公的作業の費用計算は以下の時間給に基づいて行う：

1. 中級公務員あるいは同等の職員については85ドイツマルク
2. 中の上級公務員あるいは同等の職員については105ドイツマルク
3. 上級公務員あるいは同等の職員については135ドイツマルク

4分の1時間が始まると共にこの時間給の4分の1を計算する。このほか、所轄官庁の職員による公的作業が官庁外で行われるとき、通常の作業時間外の旅行時間、あるいは所轄官庁によって特別に弁済される旅行時間について、また費用負担者に責任のある待ち時間について費用が徴収される。

（3）許可申請拒否あるいは申請取下げの場合、および許可撤回あるいは取り消しの場合、行政費用法§15が適用される。異議の完全または部分的却下については、最高、異議の対象となる行政行為に対し徴収される額までの費用を徴収することができる。却下の場合および費用決定に対してのみ行われた異議については、異議の対象の額の最高10パーセントの費用が徴収される。

§3 証明書発行の申請手続

(1) 証明書発行機関はデジタル署名法§5、1項1段により連邦身分証明書または旅券その他適当な方法で申請者の照合を行わなければならない。証明書申請には自署が必要である。申請書に申請者の署名法が付されている場合、証明書発行機関は照合と自署とをあらためて行わなくてもよい。

(2) デジタル署名法§5、2項に基づき証明書に第三者の代行権に関するデータを記載するときは、代行権を確実に証明し、その第三者の自署あるいは署名法を付した承認書を提出しなければならない。第三者には文書あるいは署名法の付されたデジタル方式で証明書の内容を教示し、§9、1項の使用禁止の可能性を知らせなければならない。職業上法その他の許可は特に許可証の提示によって証明すること。

§4 申請者への教示

(1) 証明書発行機関はデジタル署名法 §6、1および3段に基づき特に以下の署名法安全を保証するための必要な措置につき申請者に教示しなければならない：

1．個人サインコードの付いたデータ媒体は個人で保管し、それを紛失したときは、直ちにサインコード証明書の使用禁止手続をとること。個人サインコードの付いたデータ媒体が不要になったとき、まだ有効ならば、それを使えないようにし、使用禁止手続をとること。

2. 個人サインコードの付いたデータ媒体に対する個人照合番号その他の照合データについては秘密を保持すること。この個人データが漏洩した場合あるいはその疑いがある場合には直ちにデータを変更すること。

3. 署名法の作成および検査、並びにサインすべきデータあるいは検査すべきサインされたデータの表現には、デジタル署名法と当省令の要求に適合し、その安全性がデジタル署名法と当省令によって証明された技術コンポーネントを使うこと。これらは不正使用に対し保護すること。

4. 証明書がデジタル署名法§7、1項No.7の制限あるいはデジタル署名法§7、2項のデータを含み、それがサインされたデータの記載事項にとって重要であるとき、証明書をデータに付し、署名法に含めること。

5. サインされたデータの使用について日時が重要である可能性が存在するとき、日付印を押すこと。

6. データが長期間にわたってサインされた形で必要な場合、§18に従って新たに署名法を付けること。

7. 署名法の検査の際、サインコード証明書と付加証明書とがサイン作成の時点で有効であったかどうか、サインコード証明書がデジタル署名法§7、1項No.7の制限を含むかどうか、また場合によってはNo.4および5が守られているか、調べること。

（2）申請者がすでに証明書を所有している場合、あらためて教示は行わなくてもよい。

§5 サインコードと照合データの作成とメモリー

(1) サインコードがサインコード所持者によって作成される場合、証明書発行機関は所持者が個人サインコードの作成およびメモリーと使用とに、デジタル署名法および当省令に従った適切な技術コンポーネントを使っているかを確認すること。

(2) サインコードが証明書発行機関によって作成される場合、証明書発行機関は個人サインコードの漏洩と証明書発行機関でのメモリーが生じないよう措置を講じること。これは個人サインコードの付いたデータ媒体に対する個人照合番号その他のサインコード所持者照合データについても当てはまる。

§6 サインコードと照合データの引渡し

証明書発行機関が§5、2 項に従ってサインコードあるいは照合データを作成するとき、サインコード所持者が書面で他の引渡し方法を希望しない限り、サインコードおよび照合データをサインコード所持者に直接引き渡し、引渡しを書面で確認させること。証明書発行機関は個人サインコードあるいはサインコード証明書を引き渡すと同時に公開サインコードを所轄官庁に引き渡すこと。

§7 証明書の有効期間

証明書の有効期間は最高 5 年とし、§17、２項による、使ったアルゴリズムとそれに属するパラメーターの適性の期間を超えてはならない。付加証明書の有効期間は遅くとも、それの属するサインコード証明書の有効期間の終了とともに終了する。

§8 証明書の公式リスト

(1) 証明書発行機関はその発行した証明書を、少なくとも§17、２項による、証明書に挙げたアルゴリズムとそれに属するパラメーターが適性を有すると判断される期間、デジタル署名法§5、1 項 2 段の規定に従ってリストに記載しなければならない。

(2) 所轄官庁はその発行した証明書をデジタル署名法§4、5 項 3 段の規定に従い 1 項に記した期間リストに記載しなければならない。これは外国の証明書が承認される場合、外国の証明書発行最高機関の公開サインコードの証明書にも適用される。リストに含まれる外国の証明書については、所轄官庁はその承認を署名法で証明すること。所轄官庁は、証明書を呼び出しできる電気通信番号およびその公開サインコードを連邦官報に公示し、証明書発行機関に直ちに知らせなければならない。

(3) 1 項に記した期限が過ぎたあと、証明書発行機関と所轄官庁とは、個々の場合申請によっ

て§13、2項に記した期間が経過するまで証明書のチェックが可能なような措置を講じなければならない。

§9 証明書使用禁止手続

(1) 証明書発行機関はサインコード所持者、およびその代行権のデータが証明書に記入されている第三者、および所轄官庁とに、いつでも証明書の使用禁止手続がとれるような電話番号を教え、それに対し確証方法をオッファしなければならない。

(2) 証明書発行機関はデジタル署名法§8 の前提のもとで、サインコード所持者あるいは 1 項によるその代行者または資格のある第三者の署名法の付された申請書あるいは書面申請書が提出されるか、あるいは合意した確証方法が適用された場合、証明書を使用禁止しなければならない。

(3) 証明書の使用禁止は日付と時刻を記入してデジタル署名法§8 のリストに記載する。撤回は許容されない。

§10 従業員の信頼性

証明書発行機関は証明書発行あるいは日付印の発行に従事する人間の信頼性を確認しなければならない。これには特に連邦中央登記法§30 による品行証明書の提出を要求することができる。信頼できない人間は証明書発行手続と日付印発行から除外しなければならない。

§11 技術コンポーネントの保護

証明書発行機関は個人サインコードおよび証明書と日付印作成に使う技術コンポーネント、証明書をチェック可能なようにしておくために使う技術コンポーネントの不正使用防止の措置を講じなければならない。

§12 安全計画

(1) デジタル署名法§4、3 項 3 段記載の安全計画はすべての安全措置、とりわけ使用した技術コンポーネントの一覧、証明書発行作業のプロセスオーガナイゼーションの説明を含まなければならない。安全にとって重大な変更があった場合には直ちに計画をそれに合わせること。

(2) 所轄官庁は適切な安全措置の施行令を備え、それを連邦官報に公表する。安全計画を立てるときにはこの措置を参考にすること。施行令は連邦情報技術安全局のデータに基づいて作成される。経済と学術の専門家の助言を求めること。

§13 ドキュメント

(1) デジタル署名法§10 によるドキュメントは、安全計画およびその変更、§15、1 項の検査報告および確認書、申請者との契約合意事項、所轄官庁から得た証明書を含むものでなくてはならない。提出された証明申請書および申請者との契約については、提示された身分証明書あるいは他の人物照合証明書のコピー、第三者のデータの記入に必要な書類、仮名の付与、義務づけられている申請者と第三者への教示、発行した証明書およびその日付と引渡し、証明書の使用禁止、デジタル署名法§12、2 項による問合せ回答を記録すること。証明書発行機関が§5、2 項のサインコードまたは照合データを作成する場合は、引渡しの時点と受取確認を記録すること。デジタル形式で行われた記録はデジタルでサインしなければならない。

(2) 1 項のドキュメントはサインコード証明書発行の時点から少なくとも 35 年間保存し、この期間使えることを保証すること。デジタル署名法§12、2 項 2 段の問合せ回答のドキュメントは 12 ヶ月保存すること。

§14 営業停止

(1) 証明書発行機関は、デジタル署名法§11、1 項に従って営業停止を行うときは、遅くとも 4 ヶ月前に所轄官庁に連絡しなければならない。

(2) 営業停止前に証明書発行機関は、使用禁止されていない、営業停止の時点でまだ有効期間の終わっていない証明書のすべてにつきサインコード所持者に、少なくとも 3 ヶ月の期限で、営業停止の意向を伝え、他の証明書発行機関がその証明書を引き継ぐかどうか、引き継ぐ場合はその名前を伝えなければならない。他の証明書発行機関が証明書を引き継がない場合、1 項に記した期間が経過すれば、この時点でまだ使用禁止されていない、あるいは有効期間の過ぎていない証明書はすべて使用禁止とし、使用禁止されるべき証明書のサインコード所持者にはそれを知らせること。

(3) 所轄官庁への通知とサインコード所持者への連絡は署名法の付いたデジタル方式あるいは文書で行う。

(4) デジタル署名法§11、2 項に従いドキュメントを引き継ぐ証明書発行機関、あるいは所轄官庁は証明書を§8、1 および 3 項のリストに載せなければならない。

§15 証明書発行機関監察

(1) 証明書発行機関は営業開始前、および安全にとって重大な変更のあと、および 2 年に 1 度の割合でデジタル署名法§4、3 項 2 段による検査手続をとり、所轄官庁に検査報告と、デジタル署名法と当省令の規定を満たしているとの確認書を提出しなければならない。

(2) 所轄官庁は適当な期間をおいて、あるいはデジタル署名法もしくは当省令の規定違反の疑いのある場合、監査を行う。

§16 技術コンポーネントへの要求

(1) サインコード作成に必要な技術コンポーネントは、コードは絶対安全に近い確率でただ1つだけ存在し、 個人サインコードは公開サインコードからは算出できないようなものでなくてはならない。個人サインコードの秘密保持は保証されていなくてはならない。またコピーできるようなものであってはならない。技術コンポーネントの安全技術上の変更は利用者にとって認識できるものでなくてはならない。

(2) 署名法の作成あるいは検査に必要な技術コンポーネントは、サインから個人サインコードが算出できないか、あるいは他の方法でサインが偽造できないようなものでなくてはならない。個人サインコードは、所持者を所有と知識によって照合してはじめて使用することが許され、使用のとき漏洩があってはならない。サインコード所持者の照合には追加手段としてバイオメトリックな標識を使うことができる。照合データの把握に必要な技術コンポーネントは、照合データが漏洩することなく、照合データ個人サインコードの付いたデータ媒体にのみメモリーされるようなものでなくてはならない。 技術コンポーネントの安全技術上の変更は利用者にとって認識できるものでなくてはならない。

(3) サインされるデータの表現に必要な技術コンポーネントは、サインする人間が、サインのおよぶデータを一義的に決定でき、署名法は彼の操作でのみ可能であり、それは前もって一義的に表示されるようなものでなくてはならない。サインされたデータの検査に必要な技術コンポーネントは、検査する人間が、サインのおよぶデータおよびサインコード所持者を一義的に確認でき、署名法の正確さが確実にチェックされ、正しく表示されるようなものでなくてはならない。証明書のチェックのための技術コンポーネントは、チェックされた証明書が記された時点に証明書のリストに載っていて、使用禁止されていないことが一義的に分かるものでなくてはならない。技術コンポーネントは、必要があれば、サインされるべきあるいはサインされたデータの内容が十分に分かるものでなくてはならない。1～4段の技術コンポーネントが営業目的で第三者に提供されるときは、データの一義的な解釈が確保され、技術コンポーネントは利用の際自動的にその真なることがチェックされなければならない。 技術コンポーネントの安全技術上の変更は利用者にとって認識できるものでなくてはならない。

(4) デジタル署名法§4、5項3段または§5、1項2段により証明書をチェック可能な状態に保つための技術コンポーネントは、権限のある者のみが記入・変更を行うことができ、証明書の使用禁止が気付かれずに撤回されことはなく、与えられた回答の真なることがチェックできるようなものでなくてはならない。回答はチェックされた証明書が証明書のリストに記載の時点に載っているか、それが使用禁止されていないかどうかの内容を含まなければならない。チェックのためにのみ保持されている証明書は一般に呼び出し可能であってはならない。技術コン

ポーネントの安全技術上の変更は操作者にとって認識できるものでなくてはならない。

(5) デジタル署名法§9 により日付印を作成する技術コンポーネントは、日付印作成の時点で通用している法定の日時が変造されることなく日付印に記されるようなものでなくてはならない。 技術コンポーネントの安全技術上の変更は操作者にとって認識できるものでなくてはならない。

(6) 所轄官庁は適切な安全措置の施行令を備え、それを連邦官報に公表する。技術コンポーネントではこの措置を参考にすること。施行令は連邦情報技術安全局のデータに基づいて作成される。経済と学術の専門家の助言を求めること。

§17 技術コンポーネントの検査

(1) デジタル署名法§14、4 項による技術コンポーネントの検査は「情報技術システムの安全性評価の基準」(省庁合同報告 1992 年、p. 545) によって行う。検査は、サインコード作成または個人サインコードのメモリーあるいは使用のための技術コンポーネントおよび営業目的で第三者に利用提供される技術コンポーネントについては少なくとも検査段階「E4」、その他では少なくとも「E2」の範囲でなければならない。安全機構の強さは「高度の」との評点、アルゴリズムとそれに属するパラメーターとは 2 項に従い適性を有するとの評点がつくものでなくてはならない。

(2) 所轄官庁は連邦官報に、サインコードの作成、サインされるべきデータのハッシュ、署名法の作成と検査に適性を有するとみなされるアルゴリズムとそれに属するパラメーターの一覧およびこの適性が通用する期限を公示する。この期限は評価と公表の時点から少なくとも 6 年とする。この適性は、署名法の発見できない偽造あるいはサインされたデータの発見できない変造が、学術と技術の水準に従えば一定の期間内には絶対安全に近い確率で起こり得ないとき、存在する。適性は連邦情報技術安全局のデータにより、国際基準を参考にして証明される。経済と学術の専門家の助言を求めること。

(3) デジタル署名法§14、4 項の技術コンポーネントへの要求が満たされていることを証明するときには、§16 のどの要求に証明が該当するか、どんな使用条件のもとで、2 項のどのアルゴリズムとそれに属するパラメーターが使われるか、それらはどの時点まで適性を保持するか、1 項のどの検査段階で技術コンポーネントは検査されたかを記すこと。検査報告と確認書は所轄官庁に一部保管すること。所轄官庁は、検査にもしくは証明された技術コンポーネントに欠陥の疑いがあるとき、および抜取方法により、技術コンポーネントが 1 項に従って検査されたか、技術コンポーネントはデジタル署名法および当省令の要求を満たしているかの鑑定を中立の第三者に依頼することができる。関係する作成者、販売者、検査機関はそれに必要な支援を与えること。この支援が与えられない場合、あるいは確認された技術コンポーネントが十分に

検査されていなかったか、あるいは要求を満たさないことが判明すれば、所轄官庁は与えた確認の無効を宣言することができる。

(4) 所轄官庁はデジタル署名法§14、4によって承認された機関、およびその機関から3項の確認を得た技術コンポーネントを連邦官報に公示し、証明書発行機関に直ちに伝えなければならない。技術コンポーネントについてはどの時点まで確認が有効かを記する。承認が取り消されるかあるいは確認の無効が宣言された場合、これも同じく連邦官報に公示し、証明書発行機関に直ちに伝えること。

§18 新しい署名法

データが、その作成と検査に使われた、§17、2項のアルゴリズムとそれに属するパラメーターが適性を有すると判断されるより長い期間サインされた形で必要である場合、そのデータにはアルゴリズムとそれに属するパラメーターの適性の期限が切れる前に新しい署名法を付けること。この新しい署名法は新しいアルゴリズムとそれに属するパラメーターで作成し、古い署名法を含み日付印を有しなければならない。

§19 発効

この省令は1997年11月1日に発効する。