電子識別規則 (EU) No 910/2014

[参考訳]

2017 年 10 月 10 日
明治大学法学部教授
夏　井　高　人

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC（OJ L 257, 28.8.2014, p.73‐114）に基づき、翻訳を試みた。テキスト（英語版）は、下記の Eur-lex の Web サイトから入手した。

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN
[2017 年 10 月 1 日確認]

この規則(EU) No 910/2014（以下「電子識別規則」という。）は、EU における個人識別データ（識別子）、電子識別、電子的な本人確認、電子署名、タイムスタンプ証明及び Web サイト証明を含め、ある対象の電子的な同一性確認のための基本法令の 1 つである。

この電子的な同一性確認は、自然人及び法人（将来的にはロボットまたは人工知能システムを含む。）のような電子文書または電子データの発行者、発行された電子文書または電子データの同一性確認だけではなく、その確認に用いられる電子証明書や関連データの同一性確認及び電子証明それ自体の同一性を含むものであるので、ある種の入れ子構造のような構造、または、循環論理的な論理構造をもっている。その意味において、論理的に「真の証明」になっているか否かに疑問があるし（後掲『電子商取引法』の第 3 章参照）、また、将来、量子コンピュータが普及した時点においてもなお、現時点と同程度の信頼性と機密性を維持できるとは全く考えられないけれども、現時点では、そのような根源的な問題に関しては疑問を挟まないことにするというのがビジネスの世界における不文律または礼儀作法の一種となっている。

そのような前提において、電子識別規則は、情報財（デジタル資産）の管理という側面においても電子識別の応用可能性があり（前文(65)参照）、それによって、EU の域内市場の活性化と EU の競争力の確保を目標としている点には注目すべきである。

電子識別規則の制定により、従前の電子署名指令 1999/93/EC は、廃止された（第 50 条参照）。

電子識別規則の第 8 条、第 9 条、第 12 条、第 17 条、第 19 条、第 20 条、第 22 条、第 23 条、第 24 条、第 27 条、第 28 条、第 29 条、第 30 条、第 31 条、第 32 条、第 33 条、第 34 条、第 37 条、第 38 条、第 39 条（準用）、第 40 条（準用）、第 42 条、第 44 条及び第 45 条によって欧州委員会が制定できるものと定められている実装法令中の主要なものは、下記の

Eur-lex の Web サイトで入手できる。

Commission Implementing Decision (EU) 2015/296
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D0296&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Decision (EU) 2015/1505
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Decision (EU) 2015/1506
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Decision (EU) 2015/1984
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1984&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Decision (EU) 2016/650
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0650&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Regulation (EU) 2015/806
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0806&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Regulation (EU) 2015/1501
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501&from=EN
[2017 年 10 月 6 日確認]

Commission Implementing Regulation (EU) 2015/1502
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=EN
[2017 年 10 月 6 日確認]

これらの実装法令に加え、関連する実装法令として、下記の法令が定められている。

Commission Implementing Decision 2014/148/EU
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:080:FULL&from=EN
[2017 年 10 月 10 日確認]

この電子識別規則の特徴の 1 つとして、インシデント発生時の回復性（resilience）を確保するための制度的な仕組みがビルトインされているという点をあげることができる（第 19 条参照）。日本国の関連法令中においては、データやシステムが攻撃を受けて崩壊することがあり得ることを前提とした上で、そのような破綻的状況から一刻でも早く回復するための制度的な仕組みを内包させた法令は、極めて少ない。

同様に、インシデントの発生により、利用者等に損害が発生した場合、直接の信頼サービスプロバイダだけではなく、最終的な監督権限をもつ国（構成国）も損害賠償責任を負うこと、また、監督権限者が適格であるとの保証を与えた信頼サービスプロバイダに事故が発生し、損害賠償責任が問題となる場合、無過失の立証責任を当該プロバイダに負わせている点にも注目すべきである（第 13 条参照）。

同様の立証責任の転換条項は、一般データ規則（GDPR）の中にも見られるものであり、今後、消費者が被害を受け得る機能やサービスの提供と関連する事象に関しては、かなり広範かつ一般的なものとして立証責任の転換の仕組みが導入される可能性が極めて高いと予測可能である。このような制度的な仕組みを日本国の法制の中に導入することについては抵抗感をもつ企業が少なくないと考えられる。しかし、それらの企業が EU 域内で何らかのビジネスを行う場合には EU の法令が適用されることは、言うまでもないことであり、その結果として、EU 域内でのビジネスの場面では故意または過失の立証責任が転換されている可能性があることを常に念頭に置くべきである。そして、EU において立証責任が転換されている事象に関しては、法解釈論の問題として、過失の一応の推定の法理の適用を含め、実質的な意味で立証責任を転換するような解釈・運用が裁判所によって導入され得ることを理解すべきであろう。

一般に、立証責任の転換は、制定法の条項のみによって行われるものではなく、公平の原理に従い、比較法的な検討の結果を踏まえ、法律上の条項の解釈・運用によっても認められ得るものである。それゆえ、実質的な公平及び利益衡量の観点を完全に捨象した純粋に形式論理だけのものという意味での要件事実論のみに依拠することは、少なくとも企業法務のあり方としては、極めてリスキーなことである。

電子識別規則は、前文、条文及び別紙の 3 つの部分で構成されている。この参考訳においては、前文、条文及び別紙の全文を訳出した。

この参考訳においては、原則として直訳とした。直訳のままでは日本語として意味の通らない部分や非常にわかりにくい部分に関しては、やむを得ず意訳とした。

ただし、意訳の語彙上の選択基準は、個々の法令の制定趣旨や当該法令の起草者の個人的趣味や歴史的変遷等を反映せざるを得ない部分があるので、個々の法令により一定せず、常に個別的なケースバイケースの検討が求められる。それゆえ、一般の英語教育上の慣例や翻訳家の慣例とは異なる訳となっている部分がある。

この参考訳は、あくまでも電子識別規則の私的な和訳であり、関連分野の研究者のための参考として提供するものである。確定訳ではなく、現時点における検討結果の一部を示すものであるので、今後、必要に応じて改訂・修正が加えられる可能性がある。誤記等があると

きは、随時、法と情報雑誌上においてその正誤を公表する。

この参考訳に訳注はない。脚注は、全て原注である。

なお、明治大学法学部の科目である「専門演習（法情報学）」において、2017 年度秋期（2017 年 9 月～2018 年 1 月）の授業・演習課題として、電子識別規則の原文（英語版）を提示し、その翻訳文を提出させ、関連事項について質疑応答をし、夏井から解説を行った。この参考訳は、その際の学習指導のために夏井が作成・使用した参考訳文及び解説訳文を見直し、更に手を入れて再構成したものである。

（この参考訳を作成する際に考慮した事項）

「identification」は、「識別子（ID）」を意味する場合と「識別」を意味する場合とがある。この参考訳においては、文脈に即して、適宜訳し分けることにした（第 3 条(1)ないし(5)参照）。

「authentication」は、一般に、広く「認証」のことを指す場合もあるが、この電子識別規則においては、一方において、電子的な識別子（ID）と関係付けられた「本人確認」、または、電子識別システムによる「本人確認」のことを意味するものとして用いられ、他方において、電子文書及び電子データの完全性及び原本性の確認のことを意味するものとしても用いられている。そこで、それら両者を統合する語で表現する必要が生じるため、この参考訳においては、単に「確認」と訳すことにした。このように訳す場合、「verification」との区別がつかなくなるという難点があるため、「verification」に関しては、「検証」と訳すことにし、区別できるようにした。同様に、「certification」に関しては、文脈により、「認証」または「証明」と訳すことにした。

「本人確認」を意味する場合における「本人」とは、自然人の場合と法人の場合とを含む（第 3 条(5)参照）。「本人確認」の法的意義及び問題点に関しては、松本恒雄・齋藤雅弘・町村泰貴編『電子商取引法』（勁草書房、2013）の分担執筆部分である第 3 章「本人認証」（76～116 頁）で述べたとおりである。また、電子的な証明一般に関しては、夏井高人『電子署名法ー電子文書の認証と運用の仕組みー』（リックテレコム、2001）で述べたとおりである。

また、「electronic」のかかり具合が不明瞭な文が多いけれども、文脈から明らかに電子的な確認のみを指し、非電子的な確認を除外していると理解すべき部分に関しては、直接に「electronic authentication」と明示されていなくても、「電子確認」と訳した箇所がある。

他方、「website authentication」には、やや面倒な問題がある。直訳すると、「Web サイト確認」になるのであるが、日本語として違和感があるため、一般的には「Web サイト証明」と訳されている。しかし、この「Web サイト証明」にも問題がある。例えば、「certificates for website authentication」では、「Web サイト証明の証明書」となり、日本語として冗長過ぎるという問題が発生するのである。これを「Web サイト確認の証明書」と訳すとすれば、冗長性の問題は、解消する。そこで、この参考訳では、一般的な訳語とはかなり異なるが、「website authentication」を「Web サイト確認」と訳すことにした。

「identity」は、同一性の証明対象または証明手段としての「識別」または「同一性識別」を意味する場合と、属性値としての「同一性」を示す場合の両方で用いられている。「識別」または「同一性識別」を意味する場合には「identification」と同義であり得る。しかし、「identity」は、単なる一般的な識別子ではなく、特に、自然人の本人確認または法人の存在確認の際における同一性を示す概念を表象するシンボルという意味での「識別子」を指す場合に用いられると理解することができる。

一般に、このような異なる意味または機能をもつという点を明確に認識しない場合には、「identity」をうまく訳すことができず、「アイデンティティ」とカタカナ表記する例や「ID」と訳す例もある。しかし、特に後者の「ID」は、具体的な識別手段であるパスポートや身分証明書のような「identification」の略称として用いるべきものであるので、適切ではない。

この参考訳においては、文脈に応じて、「identity」を「同一性」または「同一性識別」等と訳し分けることにした。

「identity assurance level」は、「同一性保証レベル」と訳すことにした。これは、特定の識別手段の信頼性の程度を示す尺度（指標）であり、「低（low）」、「十分（substantial）」及び「高（high）」に区分される。「lower」または「higher」は、「substantial」を基準として評価され、その「substantial」の基準を定めるのが電子識別規則の目的である。

「relying party」とは、要するに、電子識別の仕組み（特に電子証明書）に依拠して電子確認の利益を受ける利用者のことを意味する（第 3 条(6)参照）。定訳はない。この参考訳では、慣例に従い、「証明書利用者」と訳すことも検討した。しかし、特に法人の場合、自然人が個別に関与することなく、電子的な自動処理が大量に実行されることに鑑み、実体的にではなく関係的に表現できる訳語のほうが望ましいとの判断から、とりあえず、「依拠者」と訳すことにした。「依拠者」との訳語では違和感がある場合には、「リライングパーティ」とカタカナ表記するのが妥当であろう。

なお、「利用者」との訳語は、一般的には可能な範囲内にある訳語の 1 つである。しかし、単なる利用者（user）との識別が不可能になるという難点があるため、この参考訳においては、「relying party」を「利用者」と訳すことを避けることにした。

「advanced electronic signature」には様々な訳があり、一定していない。この参考訳においては、月並みではあるが、便宜、「advanced electronic signature」を「高度電子署名」と訳すことにした。

「qualified electronic signature」には様々な訳があり、一定していない。しかし、日本国政府の関連委員会及び JIPDEC では「適格電子署名」との訳語を採用していることから、この参考訳においては、この訳語を尊重し、「qualified electronic signature」を「適格電子署名」と訳すことにした。

「qualified certificates」には様々な訳があり、一定していない。この参考訳においては、この訳語を尊重し、「qualified certificates」を「適格証明書」と訳すことにした。

「interoperability」は、ある技術と別の技術との間に互換性があり、個別の変換処理等を経ないで運用できる状態となっていることを意味する。種々の訳があるが、この参考訳においては、「interoperability」を「相互運用性」と訳すことにした。ただし、部分的に、「相互運用できること」等と訳した箇所がある。

「security」は、主として、無権限のアクセスやデータ改竄、データ漏洩またはシステム障害を発生させるサイバー攻撃からシステム、データ及び処理を守るための技術的な要求のことを指す。この参考訳においては、文脈に応じて、「セキュリティ」、「安全性」、「防護」等と訳し分けることにした。

「status」は、ある特別の状態にあることを意味する。「状態」または「地位」と訳すこともできるが、この参考訳においては、慣例に従い、「status」を「ステータス」とカタカナ表記することにした。

「time source」は、ある特定の時刻の最初の根拠となるデータの発生源のことを意味する。太陽、月または星の運行の人間による観測のみが発生源になっている場合、その観測者である人間が「time source」となる。幾つかの古代社会において、神官等は、そのような役割を担うことによって計画的な農耕を可能なものとし、武力をもたなくても権力者にとりいることができたと想像可能である。『禮記』の中で示されているような君主の季節儀礼や時の太鼓は、このような特別の知識と技能をもつ天官または神官の示唆に基づくものであったろうと推測される（夏井高人「『荀子』の蘭(2)」らん・ゆり 450 号 17～44 頁(2015)及び同「『荀子』の蘭（3・完）」同誌 451 号 25～52 頁(2015)参照）。現代社会では、人間の天文観測者ではなく、原子時計（atomic clock）等の物理装置によって時刻の基礎データを得ることが普通となっている。その場合、その時刻の基礎データを発生させる物理装置が「time source」となる。

この参考訳においては、慣例に従い、「time source」を「タイムソース」とカタカナ表記することにした。

「Implementing acts」は、電子識別規則においては、全ての箇所において、実装細則（施行細則）である法令（手続準則）のことを指すものとして用いられている。これは、法規範（法令）の一種である。それゆえ、この参考訳においては、「Implementing acts」を、「実装行為」ではなく、「実装法令」と訳すことにした。

「procedural arrangements」は、上述の実際に制定された委員会実装規則及び実装規則の体裁及び内容から、「手続準則」と訳すのが最も妥当であると判断した。

一般に、「arrangements」は、非常に多義的であり、文脈及び意味内容に即して訳し分ける必要があり、この参考訳においてもそのようにした。

「procedure」は、現時点における他の実装法令（施行細則）における用例との整合性等の観点を考慮に入れた上で、一律に「手続」と訳すことにした。しかし、文脈から、日本語としては「手順」と訳すほうが合理的ではないかと考えられる箇所（特に安全性確保と関連する条項）もあり、今後、更に検討を要する。

なお、一般に、「手順」であることを英語によって明確に示す場合には、「procedure」ではなく、「protocol」が用いられる。

（訳出済みの関連法令等及び参考文献）

IMI 規則(EU) No 1024/2012 の参考訳は、法と情報雑誌 2 巻 9 号 93～114 頁にある。委員会決定 2008/49/EC の参考訳は、法と情報雑誌 2 巻 9 号 84～92 頁にある。ITS 指令 2010/40/EU の参考訳は、法と情報雑誌 2 巻 9 号 27～47 頁にある。NIS 指令(EU) 2016/1148 の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 120～163 頁にある。指令 2013/40/EU の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 164～184 頁にある。指令(EU) 2017/541 の参考訳は、法と情報雑誌 2 巻 8 号 1～29 頁にある。指令(EU) 2017/541 による一部改正後の理事会決定 2005/671/JHA の参考訳は、法と情報雑誌 2 巻 8 号 38～40 頁にある。規則(EU) 2016/399（シェンゲンボーダーコード）の参考訳は、法と情報雑誌 2 巻 7 号 1～82 頁にある。規則(EU) 2016/1624 の参考訳は、法と情報雑誌 2 巻 6 号 1～98 頁にある。規則(EU) 2017/458 の参考訳は、法と情報雑誌 2 巻 7 号 83～96 頁にある。VIS 規則(EC) No 767/2008 の参考訳は、法と情報雑誌 2 巻 5 号 1～59 頁にある。PNR 指令(EU)2016/681 の参考訳は、法と情報雑誌 2 巻 3 号 119～155 頁にある。API 指令 2004/82/EC の参考訳は、法と情報雑誌 2 巻 5 号 60～70 頁にある。INSPIRE 指令 2007/2/EC の参考訳は、法と情報雑誌 2 巻 9 号 1～25 頁にある。

規則(EC) No 45/2001 の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 111～146 頁にある。個人データ保護指令 95/46/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 332～365 頁にある。指令 2002/58/EC の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 158～187 頁にある。規則 (EU) 2016/679（一般データ保護規則）の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 188～331 頁にある。

渡航文書不正防止行動計画（COM/2016/0790）の参考訳は、法と情報雑誌 2 巻 9 号 473～488 頁にある。ハイブリッドな脅威報告書（JOIN (2017) 30）の参考訳は、法と情報雑誌 2 巻 8 号 91～119 頁にある。

この参考訳を作成するに際しては、上記各参考訳の冒頭部分に掲記した文献のほか、町村泰貴・白井幸夫編『電子証拠の理論と実務－収集・保全・立証』（民事法研究会、2016）、経済産業省「平成 27 年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））調査報告書」（平成 28 年 3 月 25 日）、みずほ情報総研株式会社「平成 28 年度サイバーセキュリティ経済基盤構築事業（電子署名・認証業務利用促進事業（電子署名及び認証業務に関する調査研究等））報告書」（2017 年 3 月）、植月献二「EU 欧州デジタルアジェンダ：2013-2014 年の重点分野」外国の立法 254-2 号 (2013)、Arno R. Lodder & Andrew D. Murray (Eds.), EU Regulation of E-Commerce: A Commentary, Edward Elgar (2017)、Jeffrey Belson, Certification and Collective Marks: Law and Practice, Edward Elgar (2017) を参考にした。

＊＊＊

域内市場における電子的なやりとりのための電子識別及び信頼サービス並びに指令 1999/93/EC の廃止に関する欧州議会及び理事会の 2014 年 7 月 23 日の規則 (EU) No 910/2014

欧州議会及び欧州連合の理事会は、
欧州連合の機能に関する条約、及び、とりわけ、その第 114 条に鑑み、
欧州委員会からの提案に鑑み、
立法案を構成国の議会に送付した後、
欧州経済社会委員会の意見書に鑑み[1]、
通常の立法手続に従って審議し[2]、
以下のとおりであるので、この規則を採択する。

(1) オンライン環境において信頼を構築することは、経済及び社会の発展にとっての鍵である。とりわけ、法的安定性の欠如が認識されることによる信頼の欠如は、消費者、企業及び行政機関に対し、取引を電子的に行い、新たなサービスを導入することを躊躇させてしまうことになる。
(2) この規則は、市民、企業及び行政機関の間の安全な電子的なやりとりのための共通基盤を提供することによって、域内市場における電子的なやりとりにおける信頼を拡大すること、それによって、欧州連合内における私的なオンラインサービス及び公的なオンラインサービス、電子的な企業活動並びに電子商取引の有効性を向上させることを目指している。
(3) 欧州議会及び理事会の指令 1999/93/EC[3]は、安全であり、信頼性があり、かつ、使いやすい電子的なやりとりのための国境を越え、分野を超える包括的な枠組みを提供することなく、電子署名を取り扱っている。この規則は、同指令の法規範を拡張・拡大する。
(4) 2010 年 8 月 26 日の欧州委員会通知「欧州のためのデジタルアジェンダ」は、デジタル経済の本来の循環の主要な障碍として、デジタル市場における断片化、相互運用性の欠如及びサイバー犯罪の増加を指摘した。「EU 市民の権利に対する障碍の除去」と題する EU 市民報告書 2010 の中で、欧州委員会は、EU の市民がデジタル単一市場及び国境を越えるデジタルサービスの利益を享受することの妨げとなっている主要な諸問題を解決すべき必要性を更に強調した。
(5) 2011 年 2 月 4 日及び 2011 年 10 月 23 日の欧州理事会決議の中で、欧州理事会は、欧州委員会に対し、2015 年までにデジタル単一市場を構築すること、デジタル経済の

[1] OJ C 351, 15.11.2012, p.73.
[2] 欧州議会の 2014 年 4 月 3 日付け意見書（官報未登載）及び理事会の 2014 年 7 月 23 日付け決定
[3] 電子署名のための欧州共同体の枠組みに関する欧州議会及び理事会の 1999 年 11 月 13 日の指令 1999/93/EC（OJ L 13, 19.1.2000, p.12）

鍵となる分野における発展の速度を上げること、そして、安全な電子識別及び確認を促進することに特別に注意を払いつつ、オンラインサービスの国境を越える利用を容易なものとすることによって、完全に統合されたデジタル単一市場を促進することを勧奨した。

(6) 2011 年 5 月 27 日の理事会決議の中で、理事会は、欧州委員会に対し、電子識別、電子文書、電子署名及び電子配達サービスのような、国境を越える鍵となる実現手段のための、並びに、欧州連合全域にわたる電子政府サービスの相互運用性のための適切な条件を設けることによって、デジタル単一市場に貢献することを勧奨した。

(7) 欧州議会は、電子商取引のための域内市場の達成に関する 2011 年 9 月 21 日の決議[1]において、電子サービスの安全性、とりわけ、電子署名の安全性が重要であること、及び、汎欧州レベルの公開鍵インフラを設ける必要があることの重要性を強調し、そして、欧州委員会に対し、電子署名の国境を越える相互運用性を確保し、かつ、インターネットを使用して行われるやりとりの安全性を向上させるための欧州認証機関のゲートウェイを構築することを求めた。

(8) 欧州議会及び理事会の指令 2006/123/EC[2]は、構成国に対し、隔地者間で、かつ、電子的な手段により、適切な確認のある適切な PSC を介して、サービス活動へのアクセス及びその実施と関係する全ての手続及び方式が容易に達成され得ることを確保するための「単一の連絡場所」（PSC）を確立することを求めた。PSC を介してアクセスすることのできるオンラインサービスの多くは、電子識別、電子確認及び電子署名を必要とする。

(9) 多くの場合において、市民らは、彼らの国における国内電子識別スキームが他の構成国において承認されないという理由により、別の構成国において彼ら自身を確認するための彼らの電子識別を用いることができない。電子的な障壁は、サービスプロバイダが、域内市場における利益を完全に享受することを妨げている。電子識別の相互承認は、域内市場内の無数のサービスの国境を越える提供を容易なものとし、かつ、企業が、行政機関との交渉における多数の障碍と直面することなく、国境を越えることを基本とした業務遂行を可能とすることであろう。

(10) 欧州議会及び理事会の指令 2011/24/EU[3]は、e-health について職責を負う国内機関のネットワークを設置した。国境を越える医療の安全性及び継続性を拡大するために、そのネットワークは、「国境を越える医療におけるデータの移転性を促進するための共通の識別及び確認手段」を支援することを含め、電子的な医療データ及びサービスへの国境を越えるアクセスに関する運用指針を作成することを求められている。電子識別及び電子確認の相互承認は、欧州の市民のための国境を越える医療を現実のものとするための鍵である。人々が診療を求めて旅行する場合、彼らの医療データは、診療をする国の中でアクセス可能である必要がある。それは、堅固であり、安全であり、かつ、信頼できる電子識別の枠組みを求める。

---

[1] OJ C 50 E, 21.2.2012, p.1.

[2] 域内市場におけるサービスに関する欧州議会及び理事会の 2006 年 12 月 12 日の指令 2006/123/EC（OJ L 376, 27.12.2006, p.36）

[3] 国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU（OJ L 88, 4.4.2011, p.45）

(11) この規則は、欧州議会及び理事会の指令 95/46/EC[1]に定める個人データ保護に関する基本原則を完全に遵守して適用される。この点に関し、この規則により確立される相互承認の基本原則との関連で、オンラインサービスのための確認は、当該オンラインサービスへのアクセスを与えるために十分であり、関連性があり、かつ、過剰ではない識別子のみの処理と関係する。更に、指令 95/46/EC に基づく処理の機密性及び安全性と関係する義務は、信頼サービスプロバイダ及び監督機関によって尊重されなければならない。

(12) この指令の目的の 1 つは、少なくとも、公的サービスのために、構成国内において確認のために使用される電子識別手段の国境を越える利用に対する既存の障碍を除去することである。この規則は、構成国内において構築された電子的な同一性管理システム及び関連インフラに関して干渉することを狙いとするものではない。この規則の狙いは、構成国によって提供される国境を越えるオンラインサービスへのアクセスのために、安全な電子識別及び電子確認が可能であることを確保することにある。

(13) 構成国は、オンラインサービスにアクセスするための電子的な識別の目的のための手段を使用または導入することを自由のままとされなければならない。構成国は、これらの手段の提供の中に民間部門を含めるか否かを決定することもできるものとしなければならない。構成国は、欧州委員会に対して自国の電子識別スキームを通知すべき義務を負わない。少なくとも、公的なオンラインサービスまたは特定のサービスへのアクセスのために構成国レベルで使用される電子識別スキームの全部、その中の幾つかを欧州委員会に対して通知すること、または、それを全く通知しないことの選択は、構成国に任されている。

(14) どの電子識別手段が承認されなければならないか、及び、電子識別スキームがどのようにして通知されるべきかに関し、この規則の中で幾つかの要件を定める必要がある。これらの要件は、各構成国が、構成国相互の電子識別スキームにおいて必要な信頼の構築、そして、各構成国の通知されたスキームの範囲内にある電子識別手段の相互承認を支援するものでなければならない。相互承認の基本原則は、構成国の電子識別スキームの通知が通知の要件に適合しており、かつ、その通知が EU 官報上で公示された場合に適用されなければならない。しかしながら、相互承認の原則は、オンラインサービスのための確認のみに関するものでなければならない。それらのオンラインサービスへのアクセス及びそのサービスの申込者に対する最終的な伝送は、国内立法に定める要件に基づき、そのようなサービスを受ける権利と密接に連携するものでなければならない。

(15) 電子識別手段を承認すべき義務は、その識別手段が、当のオンラインサービスのために必要なレベルと均等またはそれ以上のレベルに対応する同一性保証レベルのものであることのみと関連している。加えて、この義務は、当の公的部門の組織が、当該サービスにオンラインでアクセスすることとの関係において、「十分（substantial）」または「高（high）」の保証レベルを使用する場合においてのみ適用されるものとしなければな

[1] 個人データの処理と関連する個人の保護及びそのデータの支障のない移転に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令 95/46/EC（OJ L 281, 23.11.1995, p.31）

らない。構成国は、欧州連合の法律に従い、より低い同一性保証レベルの電子識別手段を承認することは、自由のままとされなければならない。

(16) 保証レベルは、個人の同一性を確認し、そして、特定の識別子の識別を求める者が実際に当該同一性を割り当てられた者の同一性であることの保証を提供する際の電子識別手段の信頼性の程度を特徴付けるものでなければならない。その保証レベルは、処理（例えば、同一性の証明及び検証並びに確認）、管理活動（例えば、電子識別手段を発行する組織及びそのような手段を発行する手続）並びに実装された技術上の管理を考慮に入れた上で、ある者から識別を求められている、または、ある者に割り当てられた同一性に電子識別手段が提供する信頼性の程度に依拠する。欧州連合の資金による Large-Scale Pilots、標準化及び国際活動の結果として、保証レベルについての様々な技術的な定義及び記述が存在する。とりわけ、Large-Scale Pilot STORK 及び ISO 29115 は、就中、レベル 2、レベル 3 及びレベル 4 を指示している。それらは、特に、適格証明書を発行するための同一性の証明に関し、レベル高（level high）の保証と関連するこの規則の一貫性のある適用を確保しつつ、この規則の意味における低、十分及び高の各レベルの保証のための技術上のミニマムの要求事項、技術標準及び手続を定める際、考慮に入れられなければならない。定められる要求事項は、技術的に中立なものでなければならない。異なる技術を通じて必要なセキュリティ上の要求事項を達成できるものとしなければならない。

(17) 構成国は、オンラインサービスまたは電子的なやりとりに必要な場合、民間部門に対し、識別の目的のために通知されたスキームに基づく電子識別手段の任意の使用を推奨しなければならない。そのような電子識別手段を利用できることにより、民間部門を、少なくとも、公的サービスのために多数の構成国において既に広範に使用されている電子識別及び電子的な確認に依拠できるようにし、そして、企業及び市民が、国境を越えるオンラインサービスへアクセスすることをより容易なものとすることであろう。民間部門による国境を越えるそのような電子識別手段の使用を促進するために、構成国から提供される確認を受けることのできる可能性は、当該構成国内で設立された民間部門の依拠者に対して適用されるのと同じ要件に基づき、当該構成国の領土外において設立された民間部門の依拠者にとって利用可能なものとしなければならない。その結果、民間部門の依拠者に関しては、通知元である構成国は、確認手段へのアクセスの条件を定めることができる。そのようなアクセスの条件は、通知されたスキームと関連する確認手段が民間部門の依拠者に対して現実に利用可能であるか否かの情報を提供できる。

(18) この規則は、この規則に基づく関連義務の不遵守について、通知元である構成国、電子識別手段を発行する者及び確認手続を運営する者の法的責任を定める。しかしながら、この規則は、法的責任に関する国内法に従って適用される。それゆえ、この規則は、例えば、証明責任を含め、損害の定義に関する構成国の国内法令または適用可能な関連手続法令を害しない。

(19) 電子識別スキームの安全性は、電子識別手段の信頼性のある国境を越える相互承認の鍵となるものである。この文脈において、構成国は、欧州レベルにおける電子識別スキームの安全性及び相互運用性に関し、協力しなければならない。電子識別スキームが、国内レベルにおいて依拠者によって特定のハードウェアまたはソフトウェアが使用

されることを要求する場合、国境を越える相互運用性は、それらの構成国に対し、その構成国の措置で設立された依拠者に対してそのような義務及び関連費用を課すことがないことを要求する。そのような場合、相互運用性の枠組みの範囲内において、適切なソリューションが検討され、開発されなければならない。それでもなお、国内電子識別手段の固有の仕様から派生し、そのような電子的手段（例：スマートカード）の保有者を害するおそれのある技術上の要求事項は、不可避的なものである。

(20) リスクの程度に対応する高いレベルの信頼性及び安全性を育成するために、構成国による協力は、通知された電子識別スキームの技術上の相互運用性を促進するものとしなければならない。それらのスキームの相互承認のための構成国間の情報交換及びベストプラクティスの共有は、そのような協力を支援するものでなければならない。

(21) この規則は、信頼サービスの使用のための一般的な法的枠組みも構築する。しかしながら、この規則は、信頼サービスを使用し、既存の全ての信頼サービスのためのアクセスポイントをインストールすべき一般的な義務を創設するものではない。とりわけ、定められた一群の参加者の間のクローズドシステム内において専ら使用され、第三者に何らの影響も与えないサービスの提供に対しては、適用してはならない。例えば、信頼サービスを使用できるようにする内部手続を管理するために、企業内または行政機関内に設置されるシステムは、この規則の要求事項の適用対象としてはならない。第三者に対する影響をもち、公衆に対して提供される信頼サービスのみは、この規則に定める要求事項に適合するものでなければならない。国内法または欧州連合の法律によって定められた方式に関する要求事項が存在する場合、この規則のいかなる条項も、契約の締結及びその有効性またはそれ以外の法的義務と関連する側面に対して適用されることがない。加えて、この規則は、公的な登録所、とりわけ、商業登記簿及び土地登記簿にある国内法上の方式要件を害してはならない。

(22) 信頼サービスの国境を越える使用に貢献するために、全ての構成国における訴訟手続において、証拠として、信頼サービスを使用し得るものとしなければならない。この規則の中で別異に定める場合を除き、信頼サービスの法的効果を定めるのは、国内法である。

(23) この規則が信頼サービスを承認すべき義務を設ける範囲内で、そのような信頼サービスは、義務者の即時の管理外にある技術的な理由のために義務者が閲読または検証することができない場合に、排除され得るのみである。しかしながら、その義務は、それ自体としては、公的機関に対し、既存の全ての信頼サービスの技術的な閲読可能性のために必要となるハードウェア及びソフトウェアを入手すべきことを要求するものではない。

(24) この規則によってはそれらのサービスが完全に整合性のあるものとされない範囲内で、構成国は、欧州連合の法律と整合性のあるものとして、信頼サービスに関する国内法を維持または導入し得る。しかしながら、この規則を遵守する信頼サービスは、域内市場の中で支障なく循環するものでなければならない。

(25) 構成国は、国内レベルにおける適格信頼サービスとしての承認の目的のために、この規則に定める信頼サービスの非公開のリストの一部を構成するものに加え、別のタイプの信頼サービスを定めることを自由のままとされなければならない。

(26) 技術の変化の速度のゆえに、この規則は、開発に対して開かれるアプローチを採用し

なければならない。

(27) この規則は、技術的に中立のものでなければならない。規則が与える法的効果は、この規則の要求事項に適合することを条件として、何らかの技術的手段にとって達成され得るものでなければならない。

(28) とりわけ、域内市場における中小企業（SME）及び消費者の信頼を拡大するため、そして、信頼サービス及び製品の使用を促進するために、適格信頼サービス及び製品が使用または提供される場合において高いレベルの安全性を確保する要求事項及び義務を示すという観点から、適格信頼サービス及び適格信頼サービスプロバイダという概念が導入されなければならない。

(29) 理事会決定 2010/48/EC[1]によって承認された国際連合の障害者の権利に関する条約に基づく義務、とりわけ、同条約の第 9 条に沿って、障害者は、他の消費者と均等に、信頼サービス及びそのサービスの提供に際して使用されるエンドユーザ製品を使用できるものとしなければならない。それゆえ、それが可能なときは、提供される信頼サービス及びそれらのサービスの提供に際して使用されるエンドユーザ製品は、障害者にとってアクセス可能なものとされる。可能性の評価は、就中、技術的な配慮及び経済的な配慮を含めるものとしなければならない。

(30) 構成国は、この規則に基づく監督活動を行うための監督機関を指定しなければならない。構成国は、他の構成国との相互協定に基づき、当該他の構成国の領土内にある監督機関を指定することを決定できるものとしなければならない。

(31) 監督機関は、個人データ保護の法令の違反があったことが明らかである場合、例えば、適格信頼サービスプロバイダの監査結果に関してデータ保護監督機関に情報提供することによって、データ保護監督機関と協力しなければならない。情報の提供は、とりわけ、安全性の侵害及び個人データの侵害を包摂するものとしなければならない。

(32) 単一市場における利用者の信頼を増強するため、それらのプロバイダの活動と関連するリスクに対応するセキュリティ上のグッドプラクティスを適用すべき義務を、全ての信頼サービスプロバイダに対して負わせなければならない。

(33) 証明書の中における仮名の使用に関する条項は、欧州連合法または国内法により、構成国が個人の識別子を要求することを妨げてはならない。

(34) 全ての構成国は、適格信頼サービスの同等の安全性レベルを確保するための共通の防護上の基本的な要求事項に従わなければならない。欧州連合全域におけるこれらの要求事項の一貫性のある適用を容易なものとするため、構成国は、同等の手続を採用しなければならず、かつ、この分野における構成国の監督活動及びベストプラクティスに関する情報を交換しなければならない。

(35) 全ての信頼サービスプロバイダは、この規則の要求事項、とりわけ、安全性に関する要求事項、並びに、それらの業務及びサービス上のデューディリジェンス、透明性及び説明責任を確保すべき法的責任に服さなければならない。ただし、信頼サービスプロバイダによって提供されるサービスのタイプを考慮に入れた上で、それらの要求事項が関係する範囲内で、適格信頼サービスプロバイダと非適格信頼サービスプロバイダとを区

[1] 国際連合の障害者の権利に関する条約の欧州共同体による締結に関する 2009 年 12 月 26 日の理事会決定 2010/48/EC（OJ L 23, 27.1.2010, p.35）

別することが適切である。

(36) 全ての信頼サービスプロバイダについて監督体制の構築は、それらの業務及びサービスの安全性及び説明責任のための活動分野のレベル、そして、利用者の保護及び域内市場の稼働のために貢献するレベルを確保するものとしなければならない。非適格信頼サービスプロバイダは、それらのサービス及び業務の性質によって正当化されるライトタッチかつ反応的で事後的（*ex post*）な監督活動に服するものとすべきである。それゆえ、監督機関は、非適格サービスプロバイダを監督すべき一般的義務を負わない。監督機関は、（例えば、その非適格信頼サービスプロバイダ自身から、他の監督機関から、利用者もしくはビジネスパートナーからの通知によって、または、監督機関自身の調査に基づき）非適格信頼サービスプロバイダがこの規則の要求事項を遵守していないと情報を得た場合においてのみ、行動を起こすものとしなければならない。

(37) この規則は、全ての信頼サービスプロバイダの法的責任を定めるものとしなければならない。とりわけ、この規則は、それに基づき、全ての信頼サービスプロバイダが、この規則に基づく義務の不遵守によって自然人または法人に負わせた損害について賠償責任を負わなければならないとする法的責任の制度を設ける。信頼サービスプロバイダが負うべきものとなり得る財産上のリスク、または、それらを保険ポリシーによって賄う財産上のリスクの評価を促進するために、この規則は、信頼サービスプロバイダが、一定の要件の下で、それらのプロバイダが提供するサービスの使用に制限を設け、その制限を超過するサービスの使用から生ずる損害について賠償責任を負わないようにすることを認めている。消費者は、事前に、その制限に関して適正に情報提供を受けるものとしなければならない。これらの制限は、例えば、提供されるサービスの契約条項及び契約条件の中にその制限に関する情報を含めることにより、または、それ以外の認識可能な手段を介して、第三者から認識可能なものでなければならない。これらの基本原則に有効性を与える目的のために、この規則は、法的責任に関する国内法に従って適用されなければならない。それゆえ、この規則は、例えば、損害、意図、落度の定義に関する構成国の国内法令または適用可能な関連手続法令を害さない。

(38) 安全性侵害通知及びセキュリティリスク評価は、安全性の侵害または完全性の喪失の場合において関係者に十分な情報を提供するために、重要なことである。

(39) 欧州委員会及び構成国が、この規則によって導入された侵害通知の仕組みの有効性を評価できるようにするため、監督機関は、欧州委員会及び欧州ネットワーク情報セキュリティ局（ENISA）に対する要旨情報の提供を求められるものとしなければならない。

(40) 欧州委員会及び構成国が、この規則によって導入された拡大された監督の仕組みの有効性を評価できるようにするため、監督機関は、その活動に関する報告を求められるものとしなければならない。このことは、監督機関の間におけるグッドプラクティスの交換の促進において有用なものとなり得るし、また、全ての構成国における基本的な監督義務の一貫性のある効果的な実装の検証を確保し得るものである。

(41) 適格信頼サービスプロバイダの持続性及び継続性を確保するため、及び、適格信頼サービスの継続性における利用者の信頼を増強するため、監督機関は、適格信頼サービスプロバイダがその活動を終了する場合において、そのプロバイダの存否及び終了計画の条項の正確な適用を検証しなければならない。

(42) 例えば、あるプロバイダがそのサービスを別の構成国の領土内で提供しており、かつ、そのプロバイダがその国では監督に服していない場合、あるいは、プロバイダのコンピュータが、そのプロバイダが設立されている国以外の構成国の領土内に所在している場合、適格信頼サービスプロバイダの監督を促進するために、構成国内の監督機関の間の共助システムが設けられなければならない。

(43) 適格信頼サービスプロバイダ及びそれらのプロバイダが提供するサービスが、この規則に定める要求事項を遵守することを確保するために、監督機関によって適格性評価が行われなければならず、また、その適格信頼サービスプロバイダから、監督機関に対し、その評価結果である適格性評価報告書が提出されなければならない。監督機関が適格信頼サービスプロバイダに対してアドホックな適格性評価報告書の提出を要求する場合、その監督機関は、とりわけ、その決定の理由を与える義務を含め、良き行政の原則及び比例性の原則を尊重しなければならない。それゆえ、監督機関は、アドホックな適格性評価を求める決定を適正に根拠付けなければならない。

(44) この規則は、信頼サービスの高いレベルの安全性及び法的安定性を提供するための堅牢な枠組みを確保することを目途とする。これに関し、欧州委員会は、製品及びサービスの適格性評価に対処する際、それが適切なときは、適格性評価機関の認定及び製品の市場調査の要件を定める欧州議会及び理事会の規則(EC) No 765/2008[1]のような、関連する既存の欧州のスキーム及び国際的なスキームとの相乗効果を求めなければならない。

(45) 適格信頼サービスプロバイダ及びそれらのプロバイダが提供する適格信頼サービスを信頼リストの中に含めることを導かなければならない効果的な開始プロセスを可能とするために、適格信頼サービスの提供につながるデューディリジェンスを促進するという観点から、予定される適格信頼サービスプロバイダと職務権限を有する監督機関との間の事前折衝が奨励されなければならない。

(46) 信頼リストは、それが、監督の時点におけるサービスプロバイダの適格ステータスを示すものであることから、市場関係者の間における信頼を構築する上で、重要な要素である。

(47) オンラインサービスにおける信頼性及びその利便性は、利用者にとって、電子サービスの利益を完全に享受し、意識的に依拠するために重要である。この目的のために、EU 信頼マークが、適格信頼サービスプロバイダによって提供される適格信頼サービスを識別するために設けられる。そのような適格信頼サービスのための EU 信頼マークは、適格信頼サービスプロバイダを別の信頼サービスと明確に区別するものであり、市場における透明性に寄与することであろう。適格信頼サービスプロバイダによる EU 信頼マークの使用は、任意のものとしなければならず、また、この規則に定める以外のいかなる要求事項も導いてはならない。

(48) 委員会決定 2009/767/EC[2]の文脈におけるような特別の場合においては、電子署名の

[1] 認定及び製品のマーケティングと関連する市場調査の要件を定め、規則(EEC) No 339/93 を廃止する欧州議会及び理事会の 2008 年 7 月 9 日の規則(EC) No 765/2008（OJ L 218, 13.8.2008, p.30）

[2] 域内市場のサービスに関する欧州議会及び理事会の指令 2006/123/EC に基づく「連絡部局」を介する電子的手段による手続の利用促進措置を定める 2009 年 10 月 16 日の委員会決定 2009/767/EC

相互承認を確保するために、高いレベルの安全性が必要となるが、より低い安全性保証のある電子署名も認められなければならない。

(49) この規則は、電子署名は、それが電子的な方式によるものであること、または、それが適格電子署名の要求事項に適合しないことのみを理由として、法的効果を否定してはならないという原則を確立しなければならない。ただし、この規則の中に定められ、それに従って適格電子署名が手書きの書面と均等な法的効果をもつものとしなければならない要求事項を除き、電子署名の法的効果を定めるのは、国内法である。

(50) 構成国の職務権限を有する機関は、現在、その文書に電子的に署名をするために、異なるフォーマットの高度電子署名を使用しているので、電子的に署名された文書を構成国が受信する際、少なくとも、数多くの高度電子署名のフォーマットが構成国によって技術的にサポートされ得ることを確保する必要がある。同様に、構成国内の職務権限を有する機関が高度電子シールを使用する場合、その機関が、少なくとも、多数の高度電子シールのフォーマットをサポートすることを確保する必要がある。

(51) 署名者のみが彼の電子署名作成データの使用に対する管理をもつことを確保するための適切な仕組み及び手続が実装されており、かつ、その機器の使用が適格電子署名の要求事項に適合している限り、署名者が、適格電子署名作成機器を第三者に託すことができるものとしなければならない。

(52) その多大な経済的利益に照らし、電子署名作成環境が署名者の代わりに信頼サービスプロバイダによって管理されている場合において、リモート電子署名の作成が増加している。しかしながら、そのような電子署名が、利用者自身が完全に管理する環境内で作成された電子署名と同じ法的承認を受けるためには、リモート電子署名サービスプロバイダは、その電子署名作成環境が信頼性のあるものであり、かつ、署名者の管理下においてのみ使用されることを保証するための、管理上及び業務遂行上の特別の安全性手続を適用し、かつ、信頼性のあるシステム及び製品を使用しなければならない。リモート電子署名作成機器を使用して適格電子署名が作成された場合、この規則に定める適格信頼サービスプロバイダに適用される要求事項が適用される。

(53) 適格証明書の停止は、多数の構成国における信頼サービスプロバイダの業務運営上の確立された実務である。それは、破棄とは異なるもので、証明書の有効性の一時的な喪失を伴うものである。法的安定性は、証明書の停止ステータスが常に明確に表示されることを求める。その目的のために、信頼サービスプロバイダは、証明書のステータス、及び、停止の場合には、証明書が停止された期間を明確に表示すべき責任を負わなければならない。この規則は、信頼サービスプロバイダまたは構成国に対して停止を使用する義務を負わせるものではないが、そのような実務を利用可能な場合及び場所においては、透明性のある規定を定めなければならない。

(54) 適格証明書の国境を越える相互運用性及び承認は、適格電子署名の国境を越える承認のための前提条件である。それゆえ、適格証明書は、この規則に定める要求事項を超える強制的な要求事項に服すものとしてはならない。ただし、国内レベルにおいては、そのような特別の属性が、適格証明書及び電子署名の国境を越える相互運用性及び

（OJ L 274, 20.10.2009, p.36）

承認を妨げないことを条件として、例えば、ユニークな識別子のような、特定の属性を適格証明書の中に含まることが認められる。

(55) ISO 15408 のような国際標準及び関連評価手法並びに相互承認覚書に基づく IT セキュリティ認証は、適格電子署名作成機器の安全性を検証するための重要なツールの 1 つであり、奨励されなければならない。しかしながら、モバイル署名及びクラウド署名のような革新的なソリューション及びサービスは、適格電子署名作成機器のための、安全性の技術標準がまだ利用可能ではなく、または、最初の IT セキュリティ認証が現在進行中である技術上及び組織条のソリューションに依拠している。そのような安全性の技術標準が利用可能ではない場合、または、最初の IT セキュリティ認証が現在進行中である場合においてのみ、そのような適格電子署名作成機器の安全性レベルは、代替的なプロセスを使用することによって評価され得る。これらのプロセスは、その安全性レベルが均等なものである限り、IT セキュリティ認証のための技術標準と同等のものでなければならない。これらのプロセスは、相互評価によって促進され得る。

(56) この規則は、適格電子署名作成機器について、高度電子署名が機能することを確保するための要求事項を定めなければならない。この規則は、そのような機器が運用されるシステム環境全体に対して適用してはならない。それゆえ、適格署名作成機器の認証の適用範囲は、署名作成機器の中で作成され、記録保存され、または、処理される署名作成データの管理及び保護のために使用されるハードウェア及びシステムソフトウェアに限定されなければならない。関連する技術標準の中で詳細に定められているので、認証義務の適用範囲は、署名作成アプリケーションを除外するものとしなければならない。

(57) 署名の有効性に関する法的安定性を確保するために、適格電子署名のコンポーネントを指定することが重要であり、それは、有効性確認を行う信頼性のある者によって評価されなければならない。更に、自分自身では適格電子署名の有効性確認を行うことを望まず、または、そうすることができない依拠者に対して適格有効性確認サービスを提供することのできる適格信頼サービスのための要求事項を指定することは、そのようなサービスに対して民間部門及び公的部門が投資することを促進する。両者の要素は、適格電子署名有効性確認を容易なものとするものであり、かつ、欧州連合レベルにおいて、全ての関係者のために利便性のあるものでなければならない。

(58) 法人からの適格電子シールを要するやりとりの場合、法人の権限のある代表者からの適格電子署名が均等に承認されなければならない。

(59) 電子シールは、電子文書が法人から発行されたことの証拠として、その文書の原本性及び完全性の確実性の確保を提供するものでなければならない。

(60) 電子シールの適格証明書を発行する信頼サービスプロバイダは、司法手続または行政手続の過程において国内レベルでそのような同一性識別が必要となる場合、電子シールの適格証明書が提供される法人を代表する自然人の同一性を確認できるようにするために必要となる措置を実装しなければならない。

(61) 電子署名及び電子シールの有効期間を超えた法的有効性を確保し、かつ、将来の技術的変化とは無関係にそれらが有効性確認され得ることを保証するために、この規則は、情報の長期保存を確保しなければならない。

(62) 適格電子タイムスタンプの安全性を確保するために、この規則は、高度電子シールもしくは高度電子署名の使用またはそれ以外の均等な手法の使用を要求するものとしなければならない。技術革新が、均等なレベルのタイムスタンプの安全性を確保することのできる新たな技術を導き得ることは、予見可能である。高度電子シールまたは高度電子署名以外の手法が使用される場合、適格信頼サービスプロバイダに対し、適格性評価報告書の中で、そのような手法が均等なレベルの安全性を確保するものであり、かつ、この規則に定める義務を遵守するものであることを説明する責任を負わせるものとしなければならない。

(63) 電子文書は、域内市場における国境を越える電子的なやりとりの将来的な発展にとって重要である。その文書が電子的な方式によるものであるということのみを理由として電子的なやりとりが排除されることがないようにするため、この規則は、電子文書が、電子的な方式によるものであるということのみを理由として法的効果を否定されてはならないという原則を確立する。

(64) 高度電子署名及び高度電子シールのフォーマットに対応する際、欧州委員会は、既存の実務、技術標準及び立法、とりわけ、委員会決定 2011/130/EU[1]に基づき、それを構築しなければならない。

(65) 法人から発行された文書の確認に加え、電子シールは、ソフトウェアコードまたはサービスのような、法人のデジタル資産の確認のために使用され得る。

(66) 電子登録配達サービスと関連する既存の法制度間の国境を越える承認を促進するための法的枠組みを定めることは、重要なことである。この枠組みは、新たな汎欧州電子登録配達サービスを提供する欧州連合の信頼サービスプロバイダにとって、新たな市場機会を開くものでもあり得る。

(67) Web サイト確認サービスは、Web サイトの訪問者が、その Web サイトの背後に本物の適法な組織が存立していることを保証し得る手段を提供する。確認された Web サイトを利用者が信用することになるので、これらのサービスは、オンラインで営まれる企業活動における信頼と信用の構築に貢献するものである。Web サイト確認サービスの提供及び使用は、完全に任意のものである。しかしながら、Web サイト確認が信頼を増強するための手段となるようにし、利用者に対してより良い経験を提供し、そして、域内市場における成長を拡大するために、この規則は、プロバイダ及びそのサービスについて、最小限の安全性及び損害賠償義務を定めなければならない。この目的のために、例えば、認証機関／ブラウザ・フォーラム（CA/B フォーラム）のような既存の産業界主導の取り組みの結果が考慮に入れられなければならない。加えて、この規則は、この規則の適用範囲外の Web サイトに対して確認のためのその他の手段または手法の使用を義務付けるものではなく、第三国の Web サイト確認サービスプロバイダが欧州連合内において消費者に対してそれらのプロバイダのサービスを提供することを妨げるものでもない。ただし、第三国のプロバイダは、欧州連合とそのプロバイダが設立されている国との間で国

[1] 域内市場におけるサービスに関する欧州議会及び理事会の指令 2006/123/EC に基づく職務権限を有する機関による電子的に署名された文書の国境を越える処理のためのミニマムの要件を定める 2011 年 2 月 25 日の委員会決定 2011/130/EU（OJ L 53, 26.2.2011, p.66）

際協定が締結されている場合、この規則に従って適格なものとして承認された Web サイト確認サービスのみをもつものとしなければならない。

(68) 設立に関する欧州連合の機能に関する条約（TFEU）の条項に従い、「法人」の概念は、運用者に対し、彼らの活動をおこなうために適すると彼らが考える法形式を選択する自由を認めている。従って、TFEU の意味における「法人」とは、その法形式とは無関係に、構成国の法律に基づき、または、構成国の法律によって構成される全ての組織のことを意味する。

(69) 欧州連合の機関、組織、事務局及び部局は、とりわけ、この規則の適用のある分野における既存のグッドプラクティス及び現在進行中のプロジェクトの結果に関し、行政協力の活用の目的のために、この規則の適用のある電子識別及び信頼サービスを承認することを奨励される。

(70) 柔軟かつ迅速な方法でこの規則の一定の細目的な技術的側面を補足するために、適格電子署名作成機器の認証について責任を負う機関によって適合されるべき基準に関し、TFEU 第 290 条に従って法令を採択する権限は、欧州委員会に対して委任されなければならない。欧州委員会が、その準備作業の中で、専門家レベルのものを含め、適切に行儀を行うことが重要である。欧州委員会は、実装法令を準備し起草する際、欧州議会及び理事会に対し、同時、適時かつ適切な関連文書の送付を確保しなければならない。

(71) この規則の実装のための統一的な条件を確保するために、とりわけ、この規則の中で定める一定の要求事項の遵守の推定を生じさせ得るものとして使用される技術標準の参照番号について、その実装権限は、欧州委員会に対して委任される。これらの権限は、欧州議会及び理事会の規則(EU) No 182/2011[1]に従って行使されなければならない。

(72) 委任された行為または実装法令を採択する際、欧州委員会は、電子識別及び信頼サービスの高いレベルの安全性及び相互運用性を確保するために、欧州及び国際的な標準化機関及び標準化組織、とりわけ、欧州標準化委員会（CEN）、欧州電気通信標準化機構（ETSI）、国際標準化機構（ISO）及び国際電気通信連合（ITU）によって作成された技術標準及び技術仕様を十分に考慮に入れなければならない。

(73) 法的安定性及び明確性のゆえに、指令 1999/93/EC は、廃止されなければならない。

(74) 指令 1999/93/EC を遵守して自然人に対して発行された適格証明書を既に使用している市場関係者のための法的安定性を確保するために、移行の目的のための十分な期間が与えられる必要がある。同様に、移行措置は、安全な署名作成機器、指令 1999/93/EC に従って判断された適格性、並びに、2016 年 7 月 1 日以前に適格証明書を発行する認証サービスプロバイダについて、定めるものとしなければならない。最後に、欧州委員会に対し、同日以前に実装法令及び委任された行為を採択するための措置を提供する必要がある。

(75) この規則に定める適用日は、欧州連合の法律、とりわけ、指令 2006/123/EC に基づいて構成国が既に負っている既存の義務を害さない。

[1] 欧州委員会の実装権限の行使の構成国による監視のための仕組みに関する規則及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011（OJ L 55, 28.2.2011, p.13）

(76) この規則の目的は、構成国によっては十分に達成することができず、その活動の規模のゆえに、欧州連合レベルでより良く達成し得るものであるので、欧州連合は、欧州連合条約第 5 条に定める補完性原則に従い、措置を採択することができる。同条に定める比例性原則に従い、この規則は、その目的を達成するために必要なところを越えることがない。

(77) 欧州データ保護監督官は、欧州議会及び理事会の規則(EC) No 45/2001[1]の第 28 条第 2 項に従って協議し、2012 年 9 月 27 日にその意見書を送付した[2]。

[1] 欧州共同体の機関及び組織による個人データの処理と関連する個人の保護並びにそのデータの支障のない移転に関する欧州議会及び理事会の 2000 年 12 月 18 日の規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1）

[2] OJ C 28, 30.1.2013, p.6.

第 1 章　一般規定

第 1 条　対象事項

電子識別手段及び信頼サービスの十分なレベルの安全性を目途としつつ、域内市場の適正な稼働を確保するという観点から、この規則は:

(a) 他の構成国の通知された電子識別スキームの範囲内にある自然人及び法人の電子識別手段を構成国が承認する場合における要件を定め;
(b) 信頼サービスのための規定、とりわけ、電子的なやりとりのための規定を定め;かつ、
(c) 電子署名、電子シール、電子タイムスタンプ、電子文書、電子登録配達サービス及び Web サイト確認のための認証サービスに関する法的枠組みを設ける。

第 2 条　適用範囲

1. この規則は、構成国から通知された電子識別スキーム、及び、欧州連合内で設立された信頼サービスプロバイダに対して、適用される。
2. この規則は、国内法による、または、特定の関係者間の合意による専ら閉鎖的なシステム内で使用される信頼サービスに対しては、適用されない。
3. この規則は、契約の法的効果及び有効性、または、方式と関するその他の法的義務もしくは手続上の義務に関する国内法または欧州連合法を害しない。

第 3 条　定義

この規則の目的のために、以下の定義が適用される:

(1) 「電子識別」とは、自然人もしくは法人または法人を代表する者をユニークに示す電子的な方式による個人識別データを使用する処理のことを意味し;
(2) 「電子識別手段」とは、個人識別データを含み、かつ、オンラインサービスのための確認に使用される有形及びまたは無形のユニットのことを意味し;
(3) 「個人識別データ」とは、自然人もしくは法人または法人を代表する者の同一性識別を可能にするための一群のデータのことを意味し;
(4) 「電子識別スキーム」とは、それに基づいて自然人もしくは法人または法人を代表する者に対して電子識別手段を発行する電子識別のためのシステムのことを意味し;
(5) 「確認」とは、自然人もしくは法人の電子的な識別子、または、電子的な方式によるデータの原本性及び完全性を確認できるようにする電子的な処理のことを意味し;
(6) 「依拠者」とは、電子識別または信頼サービスに依拠する自然人または法人のことを意味し;
(7) 「公的部門の組織」とは、国、地域もしくは地方の行政機関、公法によって規律される組織、または、1 もしくは複数のそのような機関または 1 もしくは複数の公法によって規律されるそのような組織によって設置される団体、または、それらの行政機関、組織もしくは団体から公的サービスを提供することを命じられ、そのような命令に基づいて行動す

る際の民間組織のことを意味し；
(8) 「公法によって規律される組織」とは、欧州議会及び理事会の指令 2014/24/EU[1]の第 2 条第 1 項(4)に定義する組織のことを意味し；
(9) 「署名者」とは、電子署名を作成する自然人のことを意味し；
(10) 「電子署名」とは、電子的な方式によるデータであって、電子的な方式により、別のデータに添付され、または、論理的に関連付けられ、かつ、その署名者によって署名のために使用されるもののことを意味し；
(11) 「高度電子署名」とは、第 26 条に定める要求事項に適合する電子署名のことを意味し；
(12) 「適格電子署名」とは、高度電子署名であって、適格電子署名作成機器によって作成され、かつ、電子署名の適格証明に基づくもののことを意味し；
(13) 「電子署名作成データ」とは、電子署名を作成するためにその署名者によって使用されるユニークなデータのことを意味し；
(14) 「電子署名の証明」とは、電子署名有効性確認データと自然人とを関係付け、かつ、少なくとも、当該の者の名前または仮名を確認する電子的な証明のことを意味し；
(15) 「電子署名の適格証明書」とは、電子署名の証明書であって、適格信頼サービスプロバイダから発行され、かつ、別紙 I に定める要求事項に適合するもののことを意味し；
(16) 「信頼サービス」とは、通常、以下で構成されるものの有効性を提供する電子サービスのことを意味し：
  (a) 電子署名、電子シールもしくは電子タイムスタンプ、電子登録配達サービス、及び、それらのサービスと関連する認証明書の作成、検証及び有効性確認、または
  (b) Web サイト確認証明書の作成、検証及び有効性確認、または
  (c) 電子署名、電子シールもしくはそれらのサービスと関連する証明書の保存；
(17) 「適格信頼サービス」とは、この規則に定める適用可能な要求事項に適合する信頼サービスのことを意味し；
(18) 「適格性評価組織」とは、規則(EC) No 765/2008 の第 2 条第 13 号に定める組織であって、同規則に従い、適格信頼サービスプロバイダ、及び、そのプロバイダが適用される適格信頼サービスの適格性評価を行う権限をもつものとして認定される組織のことを意味し；
(19) 「信頼サービスプロバイダ」とは、1 または複数の信頼サービスを、適格信頼サービスプロバイダまたは非適格信頼サービスプロバイダとして提供する自然人または法人のことを意味し；
(20) 「適格信頼サービスプロバイダ」とは、1 または複数の適格信頼サービスを提供し、かつ、監督機関によって適格であるステータスを与えられた信頼サービスプロバイダのことを意味し；
(21) 「製品」とは、信頼サービスの提供のために使用されることが予定されているハードウェアもしくはソフトウェア、または、ハードウェアもしくはソフトウェアのコンポーネントのことを意味し；

[1] 行政手続及び指令 2004/18/EC の廃止に関する欧州議会及び理事会の 2014 年 2 月 26 日の指令 2014/24/EU（OJ L 94, 28.3.2014, p.65）

(22)「電子署名作成機器」とは、電子署名の作成のために使用される構成されたソフトウェアまたはハードウェアのことを意味し；
(23)「適格電子署名作成機器」とは、別紙 II に定める要求事項に適合する電子署名作成機器のことを意味し；
(24)「シールの作成者」とは、電子シールを作成する法人のことを意味し；
(25)「電子シール」とは、電子的な方式によるデータであって、別のデータの原本性及び完全性を確保するために、電子的な方式により、その別のデータに添付され、または、論理的に関連付けられるもののことを意味し；
(26)「高度電子シール」とは、第 36 条に定める要求事項に適合する電子シールのことを意味し；
(27)「適格電子シール」とは、高度電子シールであって、適格電子シール作成機器によって作成され、かつ、電子シールの適格証明に基づくもののことを意味し；
(28)「電子シール作成データ」とは、電子シールを作成するためにその電子シールの作成者によって使用されるユニークなデータのことを意味し；
(29)「電子シールの証明」とは、電子シール有効性確認データと法人とを関係付け、かつ、当該法人の名前を確認する電子的な証明のことを意味し；
(30)「電子シールの適格証明書」とは、電子シールの証明書であって、適格信頼サービスプロバイダから発行され、かつ、別紙 III に定める要求事項に適合するもののことを意味し；
(31)「電子シール作成機器」とは、電子シールを作成するために使用される構成されたソフトウェアまたはハードウェアのことを意味し；
(32)「適格電子シール作成機器」とは、別紙 II に定める要求事項を準用して適合する電子シール作成機器のことを意味し；
(33)「電子タイムスタンプ」とは、電子的な方式によるデータであって、電子的な方式による別のデータを特定の時刻と結合し、その別のデータが当該時刻に存在したことの証明を確立するもののことを意味する；
(34)「適格電子タイムスタンプ」とは、電子タイムスタンプであって、第 42 条に定める要求事項に適合するもののことを意味し；
(35)「電子文書」とは、電子的な方式で記録保存されたコンテント、とりわけ、文または音響、視覚もしくは視聴覚の記録のことを意味し；
(36)「電子登録配達サービス」とは、第三者の間における電子的な手段によるデータの移転を可能にし、かつ、そのデータの送信または着信の証明を含め、送信されたデータの取扱いに関する証拠を提供するサービス、及び、送信されるデータを、喪失、盗取、毀損または何らかの無権限の改変のリスクから保護するサービスのことを意味し；
(37)「適格電子登録配達サービス」とは、電子登録配達サービスであって、第 44 条に定める要求事項に適合するもののことを意味し；
(38)「Web サイト確認証明」とは、Web サイトの確認を可能なものとし、かつ、その Web サイトとその証明書が発行される自然人または法人とを関係付ける証明のことを意味し；
(39)「適格 Web サイト確認証明書」とは、Web サイト確認証明書であって、適格信頼サービスプロバイダから発行され、別紙 IV に定める要求事項に適合するもののことを意味し；

(40)「有効性確認データ」とは、電子署名または電子シールの有効性確認のために使用されるデータのことを意味し;
(41)「有効性確認」とは、電子署名または電子シールが有効であることの検証及び確認の処理のことを意味する。

第 4 条　域内市場の基本原則

1. 構成国の領土内における他の構成国内で設立された信頼サービスプロバイダによる信頼サービスの提供に関し、この規則の適用範囲内にある理由のゆえに、制限が行われてはならない。
2. この規則を遵守する製品及び信頼サービスは、域内市場内において、支障なく流通させることが認められる。

第 5 条　データ処理及びデータ保護

1. 個人データの処理は、指令 95/46/EC に従って行われる。
2. 国内法に基づいて仮名に与えられる法律効果を妨げることなく、電子的なやりとりにおける仮名の使用は、禁止されない。

第 2 章　電子識別

第 6 条　相互承認

1. 国内法に基づき、または、行政実務により、ある構成国内において公的部門の組織によって提供されるサービスにオンラインでアクセスするために電子識別手段及び電子確認を用いる電子識別を要する場合、別の構成国において発行された電子識別手段は、以下の要件に適合する限り、当該サービスのオンラインの国境を越える確認の目的のために、前者の構成国内において承認される:
(a) その電子識別手段が、第 9 条により欧州委員会から公表されるリストの中に含まれている電子識別スキームに基づいて発行されていること;
(b) 当該電子識別手段の保証レベルが十分または高の保証レベルに対応するものである限り、その電子識別手段の保証レベルが、前者の構成国内において当該サービスにオンラインでアクセスするために関連する公的部門の組織から要求される保証レベルと均等またはそれよりも高い保証レベルに対応するものであること;
(c) 関連する公的部門の祖(s)きは、当該サービスのオンラインのアクセスとの関係において十分または高の保証レベルを使用するものであること。
その承認は、第 1 副項の(a)に示すリストを欧州委員会が公表した後、遅くとも 12 か月以内に行われる。
2. 第 9 条により欧州委員会から公表されるリストに含まれている電子識別手段に基づき発行され、かつ、低の保証レベルに対応する電子識別手段は、当該組織によってオンラインで提

供されるサービスの国境を越える確認の目的のために、公的部門の組織によって承認され得る。

第 7 条　電子識別スキームの通知の適格性

電子識別スキームは、以下の要件の全てに適合する限り、第 9 条第 1 項による通知をする資格をもつ:

(a) その電子識別スキームに基づく電子識別手段が:
  (i) 通知元である構成国によって;
  (ii) 通知元である構成国からの命令に基づき;または
  (iii) 通知元である構成国とは独立に、かつ、当該構成国から承認を受けて、発行されるものであり;
(b) その電子識別スキームに基づく電子識別手段が、公的部門の組織から提供され、かつ、通知元である構成国内において電子識別を要する少なくとも 1 のサービスへアクセスするために使用され得るものであり;
(c) 電子識別スキーム及びそれに基づいて発行される電子識別手段が、第 8 条第 3 項に示す実装法令の中で定められる保証レベルの少なくとも 1 つの要求事項に適合するものであり;
(d) 当の個人をユニークに示す個人識別データが、第 8 条第 3 項に示す実装法令の中で定められる関連保証レベルのための技術仕様、技術標準及び手続に従い、第 3 条の(1)に示す自然人または法人に対して、当該スキームに基づく電子識別手段が発行される時点で、割り当てられることを、通知元である構成国が確保するものであり;
(e) その電子識別手段が、第 8 条第 3 項に示す実装法令の中で定められる関連保証レベルのための技術仕様、技術標準及び手続に従い、本条の(d)に示す者に対して割り当てられることを、当該スキームに基づく電子識別手段を発行する者が確保するものであり;
(f) 通知元である構成国が、別の構成国内で設立された依拠者が電子的な方式で受信した個人識別データを確認できるようにするため、オンラインで確認を利用できることを確保するものであること。

  公的部門の組織以外の依拠者について、通知元である構成国は、当該確認へのアクセスの条件を定めることができる。公的部門の組織によって提供されるサービスと関連して行われる場合、国境を越える確認が、無料で提供されるものとすること。

  そのような要求事項が、通知された電子識別スキームの相互運用性を妨げ、または、大きく損なう場合、そのような確認を行おうとする依拠者に対して、構成国が不適切な特別の技術的要求を課してはならないこと;
(g) 第 9 条第 1 項による通知の少なくとも 6 か月前に、通知元である構成国が、別の構成国に対し、第 12 条第 7 項に示す実装法令によって設けられる手続準則に従い、第 12 条第 5 項に基づく義務の目的のために、当該スキームの記述を提供すること;
(h) その電子識別スキームが、第 12 条第 8 項に示す実装法令の中で定める要求事項に適合するものであること。

第 8 条　電子識別スキームの保証レベル

1. 第 9 条第 1 項により通知された電子識別スキームは、当該スキームに基づき発行される電子識別手段について、低、十分及びまたは高の保証レベルを指示するものとする。
2. 低、十分及び高の保証レベルは、以下の基準にそれぞれ適合するものとする:
(a) 保証レベルの低は、電子識別スキームの処理過程における電子識別手段であって、主張されまたは確認された個人の同一性における限定された程度の信頼性を提供し、技術仕様、技術標準、及び、技術上の管理を含め、それらと関連する手続によって特徴付けられ、その目的が識別子の濫用または改変のリスクを減少させるものであるものを指示する;
(b) 保証レベルの十分は、電子識別スキームの処理過程における電子識別手段であって、主張されまたは確認された個人の同一性における十分な程度の信頼性を提供し、技術仕様、技術標準、及び、技術上の管理を含め、それらと関連する手続によって特徴付けられ、その目的が識別子の濫用または改変のリスクを減少させるものであるものを指示する;
(c) 保証レベルの高は、電子識別スキームの処理過程における電子識別手段であって、主張されまたは確認された個人の同一性におけるより高い程度の信頼性を提供し、技術仕様、技術標準、及び、技術上の管理を含め、それらと関連する手続によって特徴付けられ、その目的が識別子の濫用または改変のリスクを減少させるものであるものを指示する;
3. 2015 年 9 月 18 日までに、関連する国際標準を考慮に入れ、かつ、第 2 項に従い、欧州委員会は、実装法令により、第 1 項の目的のために、電子識別手段について、保証レベルの低、十分及び高が指定される参照を付して、ミニマムの技術仕様、技術標準及び手続を定める。

これらのミニマムの技術仕様、技術標準及び手続は、以下の要素の信頼性及び品質に関する参照によって定められる:
(a) 電子識別手段の発行を求める自然人または法人の同一性の証明及び検証の手続;
(b) 求められた電子識別手段の発行の手続;
(c) それによって、その自然人または法人が、その同一性を確認するための電子識別手段を依拠者に対して使用する本人確認の仕組み;
(d) 電子識別手段を発行する組織;
(e) 電子識別手段の発行の求めに関与する上記以外の組織;並びに
(f) 発行される電子識別手段の技術上及び防護上の仕様。

これらの実装法令は、第 48 条第 2 項に示す審議手続に従って採択される。

第 9 条　通知

1. 通知元である構成国は、欧州委員会に対し、以下の情報を通知し、かつ、不適切な遅滞なく、その後の変更を通知する:
(a) 保証レベル、そのスキームに基づく電子識別手段の発行者を含め、電子識別スキーム

の記述;
(b) 以下の者にと関し、監督体制、及び、法的責任体制に関する情報:
  (i) 電子識別手段を発行する者;及び
  (ii) 確認手続を運営する者;
(c) 電子識別手段について責任を負う機関;
(d) ユニークな個人識別データの登録を管理する組織に関する情報;
(e) 第 12 条第 8 項に示す実装法令に定める要求事項にいかに適合しているかの記述;
(f) 第 7 条の(f)に示す確認の記述;
(g) 通知された電子識別手段もしくは電子確認または関係する毀損部分の停止または破棄の手配。

2. 第 8 条第 3 項及び第 12 条第 8 項に示す実装法令の適用の日から 1 年後、欧州委員会は、本条第 1 項によって通知された電子識別スキーム及びその基本情報のリストを EU 官報上で公示する。

3. 第 2 項に示す期間の経過後、欧州委員会が通知を受領したときは、当該通知の受領の日から 2 か月以内に、第 2 項に示すリストの改訂を EU 官報上で公示する。

4. 構成国は、欧州委員会に対し、構成国から通知された電子識別手段を第 2 項に示すリストから削除することの要請書を送付し得る。欧州委員会は、構成国の要請書を受領した日から 1 か月以内に、それに対応するリストの改訂を EU 官報上で公示する。

5. 欧州委員会は、実装法令により、第 1 項に基づく通知の態様、フォーマット及び手続を定めることができる。これらの実装法令は、第 48 条第 2 項に示す審議手続に従い、採択される。

第 10 条　安全性の侵害

1. 第 9 条第 1 項によって通知された電子識別スキームもしくは第 7 条(f)に示す確認が、当該スキームの国境を越える確認の信頼性を害するような態様で侵害され、または、部分的に毀損した場合、通知元である構成国は、遅滞なく、当該国境を越える確認または関係する毀損部分を停止または破棄し、かつ、他の構成国及び欧州委員会に対し、その連絡をする。

2. 第 1 項に示す侵害または毀損の問題を解消する際、通知元である構成国は、国境を越える確認を再構築し、かつ、他の構成国及び欧州委員会に対し、遅滞なく、その連絡をする。

3. 第 1 項に示す侵害または毀損の問題がその停止または破棄から 3 か月以内に解消されない場合、通知元である構成国は、他の構成国及び欧州委員会に対し、その電子識別スキームの放棄を通知する。

欧州委員会は、不適切な遅滞なく、それに対応するリストの改訂を EU 官報上で公示する。

第 11 条　法的責任

1. 通知元である構成国は、国境を越えるやりとりにおいて、意図的に、または、落度により、第 7 条の(d)及び(f)に基づく構成国の義務を遵守しなかったことにより自然人または法人に負わせた損害について、法的責任を負う。

2. 電子識別手段の発行者は、国境を越えるやりとりにおいて、意図的に、または、落度により、第 7 条の(e)に基づく義務を遵守しなかったことにより自然人または法人に負わせた損害について、法的責任を負う。
3. 確認手続の運営者は、国境を越えるやりとりにおいて、意図的に、または、落度により、第 7 条の(f)に基づく義務を遵守しなかったことにより自然人または法人に負わせた損害について、法的責任を負う。
4. 第 1 項、第 2 項及び第 3 項は、法的責任に関する国内法に従って適用される。
5. 第 1 項、第 2 項及び第 3 項は、第 9 条第 1 項により通知された電子識別スキームの範囲内にある電子識別手段が使用されるやりとりの関係者について、国内法上の法的責任を妨げない。

第 12 条　協力及び相互運用性

1. 第 9 条第 1 項により通知された国内電子識別スキームは、相互運用できるものとする。
2. 第 1 項の目的のために、相互運用性の枠組みが定められる。
3. 相互運用性の枠組みは、以下の基準に適合するものとする:
(a) 技術的に中立であることを目途とし、かつ、構成国内における電子識別のための特定の国内技術ソリューション間の差別を行わないこと;
(b) それが可能なときは、欧州の技術標準及び国際的な技術標準に従うこと;
(c) プライバシーバイデザインの原則の実装を促進すること;並びに
(d) 個人データが指令 95/46/EC に従って処理されることを確保すること。
4. 相互運用性の枠組みは、以下によって構成される:
(a) 第 8 条に基づく保証レベルと関係するミニマムの技術的要求事項の参照;
(b) 通知された電子識別スキームの国内保証レベルと第 8 条に基づく保証レベルとのマッピング;
(c) 相互運用性のミニマムの技術的要求事項の参照;
(d) 電子識別手段で入手できる自然人または法人をユニークに示すミニマムな個人識別データのセットの参照;
(e) 手続規則;
(f) 紛争解決のための準則;並びに
(g) 運用上の共通の防護標準。
5. 構成国は、以下に関して協力する:
(a) 第 9 条第 1 項により通知された電子識別スキーム及び構成国が通知する予定の電子識別スキームの相互運用性;並びに
(b) 電子識別スキームの安全性。
6. 構成国間の協力は、以下によって構成される:
(a) 電子識別スキーム、及び、とりわけ、相互運用性及び信頼レベルに関する技術的要求事項と関連する情報、経験及びグッドプラクティスの交換;
(b) 第 8 条に基づく電子識別スキームの信頼レベルの運用と関連する情報、経験及びグッドプラクティスの交換;

(c) この規則の適用範囲内にある電子識別スキームの相互評価;並びに
(d) 電子識別部門における関連する技術開発の検討。
7. 2015 年 3 月 18 日までに、欧州委員会は、実装法令により、リスクの程度に対応する高いレベルの信頼及び安全性を育成するために、第 5 項及び第 6 項に示す構成国間の協力を促進するために必要となる手続準則を設ける。
8. 2015 年 9 月 18 日までに、第 1 項に基づく要求事項の実装のための統一要件を定める目的のために、欧州委員会は、第 3 項に定める基準に従い、かつ、構成国間の協力の結果を考慮に入れた上で、第 4 項に定める相互運用性の枠組みに関する実装法令を採択する。
9. 本条の第 7 項及び第 8 項に示す実装法令は、第 48 条第 2 項に示す審議手続に従い、採択される。

第 3 章　信頼サービス

第 1 節　一般規定

第 13 条　法的責任及び証明責任

1. 第 2 項を妨げることなく、信頼サービスプロバイダは、意図的に、または、落度により、この規則に基づく義務を遵守しなかったことにより生じた損害について、法的責任を負う。
非適格信頼サービスプロバイダの意図または落度の証明責任は、第 1 副項に示す損害賠償を請求する自然人または法人が負う。
当該適格信頼サービスプロバイダが、当該適格信頼サービスプロバイダの意図または落度なく第 1 副項の示す損害が発生したことを証明しない限り、適格信頼サービスプロバイダの意図または落度が推定される。
2. 信頼サービスプロバイダが、その提供するサービスの使用上の制限を事前に消費者に対して適正に情報提供する場合であり、かつ、その制限が第三者にとって認識可能である場合、信頼サービスプロバイダは、その制限に示されるところを超えるサービスの使用から生ずる損害について、法的責任を負わない。
3. 第 1 項及び第 2 項は、法的責任に関する国内法に従って適用される。

第 14 条　国際的な側面

1. 第三国において設立された信頼サービスプロバイダによって提供される信頼サービスは、その第三国から発信される信頼サービスが、欧州連合と当の第三国または国際機関との間で TFEU 第 218 条に従って締結された協定に基づいて承認される場合、欧州連合内で設立された適格信頼サービスプロバイダによって提供される適格信頼サービスと法的に均等なものとして承認される。
2. 第 1 項に示す協定は、とりわけ、以下を確保する:

(a) 協定を締結している第三国の信頼サービスプロバイダまたは国際機関及びそれらが提供する信頼サービスが、欧州連合内で設立された適格信頼サービスプロバイダ及びそれらが提供する適格信頼サービスに適用される要求事項に適合するものであること;
(b) 欧州連合内で設立された適格信頼サービスプロバイダによって提供される適格信頼サービスが、協定を締結している第三国の信頼サービスプロバイダまたは国際機関によって提供される信頼サービスと法的に均等なものとして承認されること。

第 15 条　障害者のアクセス可能性

それが可能なときは、提供される信頼サービス及びそれらのサービスの提供に際して使用されるエンドユーザ製品は、障害者にとってアクセス可能なものとされる。

第 16 条　制裁

構成国は、この規則の違反行為に対して適用可能な制裁に関する規定を定める。適用される制裁は、効果的であり、比例的であり、かつ、抑止力のあるものとする。

第 2 節　監　督

第 17 条　監督機関

1. 構成国は、その領土内に設けられる監督機関を指定し、または、他の構成国との相互協定に基づき、他の構成国に設けられる監督機関を指定する。その機関は、指定元である構成国における職務を監督することについて職責を負う。
監督機関は、その職務を遂行するために必要となる権限及び十分な資源を与えられる。
2. 構成国は、欧州委員会に対し、それぞれが指定した監督機関の名称及び住所を通知する。
3. 監督機関の役割は、以下のとおりである:
(a) 事前（*ex ante*）及び事後（*ex post*）の監督を通じて、指定元である構成国の領土内で設立された適格信頼サービスプロバイダが、当該適格信頼サービスプロバイダ及びそれらが提供する適格信頼サービスがこの規則に定める要求事項に適合することを確保することを監督すること;
(b) 当該非適格信頼サービスプロバイダまたはそれらが提供する信頼サービスがこの規則に定める要求事項に適合していないとされる場合、それが必要なときは、事前（*ex ante*）及び事後（*ex post*）の監督を通じて、指定元である構成国の領土内で設立された非適格信頼サービスプロバイダと関係する措置を講ずること。
4. 第 3 項の目的のために、かつ、同項に定める制限に従い、監督機関の職務には、とりわけ、以下のものを含めるものとする:
(a) 第 18 条に従い、他の監督機関と協力し、かつ、他の監督機関に対して支援を提供すること;

(b) 第 20 条第 1 項及び第 21 条第 1 項に示す適格性評価報告書を解析すること;
(c) 第 19 条第 2 項に従い、安全性の侵害または完全性の喪失に関し、他の監督機関及び公衆に対し、情報提供すること;
(d) 本条第 6 項に従い、その主たる活動に関し、欧州委員会に対して報告すること;
(e) 第 20 条第 2 項に従い、監査を実施し、または、適格性評価機関に対し、適格信頼サービスプロバイダの適格性評価の実施を要請すること;
(f) 個人データ保護の法令の違反があったことが明らかである場合、とりわけ、適格信頼サービスプロバイダの監査結果に関し、遅滞なく情報提供することによって、データ保護監督機関と協力すること;
(g) 第 20 条及び第 21 条に従い、適格サービスプロバイダ及びそれらが提供するサービスに対し、適格のステータスを与え、並びに、そのステータスを取消すこと;
(h) 当該機関もまた監督機関である場合を除き、第 22 条第 3 項に示す国内信頼リストについて職責を負う機関に対し、ステータスを与える決定またはステータスを取消す決定に関して情報提供すること;
(i) 第 24 条第 2 項に従い、情報をアクセス可能な状態に維持することを含め、適格信頼サービスプロバイダがその活動を終了する場合、そのプロバイダの存否及び活動終了計画の条項の正確な適用を検証すること;
(j) 信頼サービスプロバイダに対し、この規則に定める要求事項を充足しないことの解消を要求すること。

5. 構成国は、国内法に定める要件に従い、監督機関に対し、信頼インフラを構築し、維持し、かつ、最新のものとすることを要請し得る。
6. 毎年 3 月 31 日までに、各監督機関は、欧州委員会に対し、第 19 条第 2 項に従い、信頼サービスプロバイダの前暦年の主要な活動に関する報告書を、それらのプロバイダから受領した侵害通知の要旨と共に、送付する。
7. 欧州委員会は、第 6 項に示す年次報告書を構成国が利用可能なものとする。
8. 欧州委員会は、実装法令により、第 6 項に示す報告書のためのフォーマット及び手続を定めることができる。これらの実装法令は、第 48 条第 2 項に示す審議手続に従い、採択される。

第 18 条　共助

1. 監督機関は、グッドプラクティスを交換するという観点から、協力する。
　監督機関は、他の監督機関からの正当な要請を受けたときは、監督組織の活動が一貫性のある方法で行われるようにするため、当該組織に対し、支援を提供する。共助は、とりわけ、第 20 条及び第 21 条に示す適格性評価報告書と関連する監査の実施の要請のような、情報提供の要請及び監督措置の要請を包摂し得る。
2. 支援の要請相手となる監督機関は、以下のいずれかを理由として、その要請を拒否し得る:
(a) その監督機関が、要請された支援を提供する職務権限を有しないこと;

(b) 要請された支援が、第 17 条に従って行われる監督機関の監督活動と比例的なものではないこと;
(c) 要請された支援を提供することが、この規則と適合しないおそれがあること。
3. それが適切なときは、構成国は、それぞれの構成国の監督機関に対し、他の構成国の監督機関からの職員が関与する共同調査を行うことを認めることができる。そのような共同活動のための準備及び手続は、それらの構成国の国内法に従い、関係する構成国間で合意して、これを設けることができる。

第 19 条　信頼サービスプロバイダに対する防護上の要求事項の適用

1. 適格信頼サービスプロバイダ及び非適格信頼サービスプロバイダは、それらが提供する信頼サービスの安全性に対して示されるリスクを管理するための適切な技術上及び組織上の措置を講ずる。最新の技術上の発展を考慮しつつ、それらの措置は、リスクの程度に応じたレベルの安全性を向上させるものとする。とりわけ、セキュリティ上のインシデントの影響を防止し、ミニマムなものとするため、及び、そのようなインシデントの悪影響について利害関係者に対して情報提供するための措置が講じられる。
2. 適格信頼サービスプロバイダ及び非適格信頼サービスプロバイダは、不適切な遅滞なく、かつ、いかなり場合においても、それに気づいた時から 24 時間以内に、監督機関に対し、及び、それが適切なときは、情報セキュリティについて職務権限を有する国内機関またはデータ保護監督機関のような、それ以外の関連機関に対し、信頼サービスの提供またはそのサービスの中で維持管理される個人データに重大な悪影響をもつ安全性の侵害または完全性の喪失について、通知する。

安全性の侵害または完全性の喪失が、その信頼サービスの提供を受けた自然人または法人に悪影響をあたえるおそれがあるときは、その信頼サービスプロバイダは、その自然人または法人に対し、不適切な遅滞なく、安全性の侵害または完全性の喪失について通知する。

それが適切なときは、とりわけ、安全性の侵害または完全性の喪失が複数の構成国と関係するものであるときは、通知を受けた監督機関は、関係する別の構成国の監督機関及び ENISA に対し、連絡する。

通知を受けた監督機関は、安全性の侵害または完全性の喪失を開示することが公共の利益に適うと判断するときは、公衆に対して情報提供し、または、当該信頼サービスプロバイダに対してそのようにすべきことを要求する。
3. 監督機関は、ENISA に対し、年 1 回、信頼サービスプロバイダから受けた安全性の侵害または完全性の喪失の通知の要旨を提出する。
4. 欧州委員会は、実装法令により:
(a) 第 1 項に示す措置の細目を定め;並びに
(b) 期限を含め、第 2 項の目的のために適用可能なフォーマット及び手続を定める。

これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 3 節　適格信頼サービス

第 20 条　適格サービスプロバイダの監督

1. 適格信頼サービスプロバイダは、適格性評価組織にとり、少なくとも 24 か月毎に、そのプロバイダの費用負担により、監査を受ける。その監査の目的は、その適格信頼サービスプロバイダ及びそれらによって提供される適格信頼サービスが、この規則に定める要求事項を充足していることを確認することである。その適格信頼サービスプロバイダは、その報告書を受領した後 3 業務日以内に、監督機関に対し、その監査結果である適格性評価報告書を提出する。
2. 第 1 項を妨げることなく、監督機関は、いつでも、監査を実施し、または、適格性評価機関に対し、その適格信頼サービスプロバイダ及びそれらによって提供される適格信頼サービスが、この規則に定める要求事項を充足していることを確認するために、そのプロバイダの費用負担により、その適格信頼サービスプロバイダの適格性評価を実施することを要求できる。個人データ保護の法令の違反があったことが明らかである場合、監督機関は、データ保護監督機関に対し、その監査結果について、連絡する。
3. 監督機関が、適格信頼サービスプロバイダに対してこの規則に基づく要求事項を充足しないことの解消を要求する場合、及び、当該プロバイダがしかるべく、かつ、それが適用可能な場合には、監督機関によって指定された期限内に、行動しない場合、その監督機関は、とりわけ、その不遵守の範囲、期間及び結果を考慮に入れた上で、当該プロバイダの適格のステータスを取消し、もしくは、そのプロバイダが提供する悪影響を受けたサービスを取消すことができ、かつ、第 22 条第 1 項に示す信頼リストを最新のものに更新する目的のために、第 22 条第 3 項に示す機関に対し、連絡し得る。その監督機関は、その適格信頼サービスプロバイダに対し、そのプロバイダの適格のステータスの取消しまたは関係するサービスの適格のステータスの取消しを連絡する。
4. 欧州委員会は、実装法令により、以下の技術標準の参照番号を定めることができる:
(a) 適格性評価機関の認定及び第 1 項に示す適格性評価報告書;
(b) それに基づいて適格性評価機関が第 1 項に示す適格信頼サービスプロバイダのそれらの適格性評価を行う監査規則。

これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 21 条　適格信頼サービスの開始

1. 適格のステータスをもたない信頼サービスプロバイダが、適格信頼サービスの提供を開始しようとするときは、それらは、監督機関に対し、その開始予定の通知書を、適格性評価機関から発行された適格性評価報告書と共に、提出する。
2. 監督機関は、その信頼サービスプロバイダ及びそのプロバイダによって提供される信頼サービスが、この規則に定める要求事項、とりわけ、信頼サービスプロバイダ及びそれらによって提供される信頼サービスの要求事項を遵守するものであるか否かを検証する。

監督機関が、その信頼サービスプロバイダ及びそのプロバイダによって提供される信頼サ

ービスが第 1 副項に示す要求事項を遵守するものであると判断するときは、その監督機関は、その信頼サービスプロバイダ及びそのプロバイダによって提供される信頼サービスに対して適格のステータスを与え、かつ、第 22 条第 3 項に示す機関に対し、本条の第 1 項に従う通知の後遅くとも 3 か月以内に、第 22 条第 1 項に示す信頼リストを最新のものに更新する目的のために、連絡する。

通知から 3 か月以内に検証の結論が出ないときは、その監督機関は、その信頼サービスプロバイダに対し、その遅延の理由を示し、かつ、検証の結論を出す期限を示して、連絡する。

3. 適格信頼サービスプロバイダは、第 22 条第 1 項に示す信頼リストの中に適格のステータスが表示された後、その適格信頼サービスの提供を開始できる。

4. 欧州委員会は、実装法令により、第 1 項及び第 2 項の目的のためのフォーマット及び手続を定めることができる。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 22 条　信頼リスト

1. 各構成国は、責任を負う適格信頼サービスプロバイダと関連する情報を、それらのプロバイダによって提供される適格信頼サービスと関連する情報と共に収録する信頼リストを作成し、維持管理、かつ、公表する。

2. 構成国は、自動処理に適した方式により、安全な方法で、電子的に署名またはシールされた第 1 項に示す信頼リストを作成し、維持管理し、かつ、公表する。

3. 構成国は、欧州委員会に対し、不適切な遅滞なく、国内信頼リストの作成、維持管理及び公表について職責を負う機関に関する情報、並びに、そのリストが公表される場所の詳細、その信頼リストに用いられる署名またはシールの証明書及びそれらの改訂を通知する。

4. 欧州委員会は、自動的な処理に適した電子署名または電子シールのある方式により、第 3 項に示す情報を、安全な経路を介して、公衆が利用可能なものとし得る。

5. 2015 年 9 月 18 日までに、欧州委員会は、実装法令により、第 1 項に示す情報の細目を定め、また、第 1 項ないし第 4 項の目的のために適用可能な信頼リストの技術仕様及びフォーマットを定めることができる。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 23 条　適格信頼サービスのための EU 信頼マーク

1. 第 21 条第 2 項の第 2 副行為に示す適格のステータスが第 22 条第 1 項に示す信頼リストの中で表示された後、適格信頼サービスプロバイダは、それらのプロバイダが提供する適格信頼サービスを単純で、認識しやすく、かつ、明瞭な方法で表示するために、EU 信頼マークを使用できる。

2. 第 1 項に示す適格信頼サービスのために EU 信頼マークを使用する際、適格信頼サービスプロバイダは、関連する信頼リストへのリンクがその Web サイト上で利用可能なものとされることを確保する。

3. 2015 年 7 月 1 日までに、欧州委員会は、実装法令により、適格信頼サービスのための EU 信頼マークの方式、とりわけ、表示、構成、大きさ及びデザインに関する細目を定める。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 24 条　適格信頼サービスプロバイダの要求事項

1. 信頼サービスのために適格証明書を発行する際、適格信頼サービスプロバイダは、適切な手段により、かつ、国内法に従い、その適格証明書が発行される自然人または法人の同一性を検証し、また、適用可能なときは、その特定の属性を検証する。

第 1 副項に示す情報は、適格信頼サービスプロバイダによって、直接、または、国内法に従って第三者に依拠して、以下のいずれかにより、検証される:

(a) 自然人の物理的な出頭、または、法人の代表権者の物理的な出頭によって;または
(b) 適格証明書の発行の前に、自然人の物理的な出頭、または、法人の代表権者の物理的な出頭が確保され、かつ、「十分」もしくは「高」の保証レベルに関する第 8 条に定める要求事項に適合する電子識別手段を使用して、リモートで;または
(c) (a)または(b)を遵守して発行された適格電子署名の証明書または適格電子シールの証明書によって;または
(d) 物理的な出頭の信頼性に関する均等な保証を提供する国内レベルで承認された上記以外の識別手段を使用して。均等な保証は、適格性評価機関によって確認される。

2. 適格信頼サービスを提供する適格信頼サービスプロバイダは:

(a) 監督機関に対し、その適格信頼サービスの提供における変更について、及び、その活動の終了の予定について、連絡し;
(b) 必要な専門性、信頼性、経験及び資質をもち、かつ、セキュリティ及び個人データ保護法令に関して適切な訓練を受け、かつ、欧州の技術標準または国際的な技術標準に対応する業務遂行手続及び管理運用手続を適用する職員、または、それが適切なときは、請負者を雇用し;
(c) 第 13 条による損害賠償という法的責任のリスクに関し、国内法に従い、十分な資金を維持管理し、及びまたは、適切な損害賠償責任保険を獲得し;
(d) 契約関係に入る前に、適格信頼サービスの使用を求める者に対し、明瞭かつ分かりやすい方式により、その使用上の制限を含め、当該サービスの使用と関連する契約条項及び契約条件の詳細について、情報提供し;
(e) 改変から保護される信頼性のあるシステム及び製品を使用し、かつ、それらによってサポートされる処理の技術上の安全性及び信頼性を確保し;
(f) 以下のとおりであることを検証可能な方式により、そのプロバイダに提供されるデータを記録保存するための信頼性のあるシステムを使用し:
    (i) 関連するデータが入手された者の同意がある場合においてのみ、検索のためにそのデータを公衆が利用できるものであること;
    (ii) 承認された者のみがデータを入力でき、記録保存されたデータを修正できること;
    (iii) データの真正性を点検できること;
(g) データの偽造及び盗取に対する適切な措置を講じ;

(h) 適格信頼サービスプロバイダが活動を終了した後を含め、適切な期間内は、とりわけ、訴訟手続の目的のために、及び、サービスの継続性を確保する目的のために、その適格信頼サービスプロバイダによって発行され及び記録されたデータに関する全ての関連情報を記録し、アクセス可能な状態に維持する。そのような記録行為は、電子的に行うことができる;
(i) 第 17 条第 4 項の(i)に基づき監督機関によって確認された条項に従い、サービスの継続性を確保するための最新の終了計画をもち;
(j) 指令 95/46/EC に従い、個人データの適法な処理を確保し;
(k) 適格証明書を発行する適格信頼サービスプロバイダの場合、証明書データベースを構築し、これを最新のものに維持する。

3. 適格証明書を発行する適格信頼サービスプロバイダが証明書の破棄を決定する場合、その破棄をその証明書データベースの中に記録し、そして、適時に、かつ、いかなる場合においても、要請を受けた後 24 時間以内に、その証明書の破棄の状態を公表する。その破棄は、その公表により、直ちに有効となる。

4. 第 3 項に関し、適格証明書を発行する適格信頼サービスプロバイダは、全ての依拠者に対し、それらのプロバイダから発行された適格証明書の有効性または破棄に関する情報を提供する。

5. 欧州委員会は、実装法令により、本条第 2 項の(e)及び(f)に基づく要求事項を遵守する信頼性のあるシステム及び製品のための技術標準の参照番号を定めることができる。信頼性のあるシステム及び製品がこれらの技術標準に適合するときは、本条に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 4 節　電子署名

第 25 条　電子署名の法的効果

1. 電子署名は、それが電子的な方式によるものであること、または、それが適格電子署名の要求事項に適合しないことのみを理由として、法的効果及び訴訟手続における証拠としての許容性を否定してはならない。

2. 適格電子署名は、手書きの署名と均等な法的効果をもつ。

3. ある構成国内で発行された適格証明書に基づく適格電子署名は、他の全ての構成国において、適格電子署名として承認される。

第 26 条　高度電子署名の要求事項

高度電子署名は、以下の要求事項に適合するものとする:
(a) その署名者とユニークに関連付けられるものであること;
(b) その署名者を識別できるものであること;

(c) その署名者が、彼のみの管理下で、高いレベルの信頼性をもって、使用可能な電子署名作成データを使用して作成されるものであり;かつ
(d) データ内のその後の変更が検出可能であるような方法で、署名されたデータと関連付けられるものであること。

第 27 条　公的サービスにおける電子署名

1. 公的部門の組織によって、または、その代りに提供されるオンラインサービスを利用するために、高度電子署名を構成国が要求する場合、当該構成国は、高度電子署名、電子署名の適格証明書に基づく高度電子署名、及び、少なくとも、第 5 項に示す実装法令に定めるフォーマットまたは使用方法による適格電子署名を承認する。
2. 公的部門の組織によって、または、その代りに提供されるオンラインサービスを利用するために、適格証明書に基づく高度電子署名を構成国が要求する場合、当該構成国は、適格証明書に基づく高度電子署名、及び、少なくとも、第 5 項に示す実装法令に定めるフォーマットまたは使用方法による適格電子署名を承認する。
3. 構成国は、公的部門の組織によって提供されるオンラインサービスにおける国境を越える使用について、適格電子署名よりも高い安全性レベルの電子署名を要求してはならない。
4. 欧州委員会は、実装法令により、高度電子署名のための技術標準の参照番号を定めることができる。高度電子署名がこれらの技術標準に適合する場合、本条第 1 項及び第 2 項並びに第 26 条に示す高度電子署名の要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。
5. 2015 年 9 月 18 日までに、かつ、既存の実務、技術標準及び欧州連合の法的行為を考慮に入れた上で、欧州委員会は、実装法令により、高度電子署名の参照フォーマットまたは代替的なフォーマットが使用される場合の参照手段を定めることができる。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 28 条　電子署名の適格証明書

1. 電子署名の適格証明書は、別紙 I に定める要求事項に適合するものとする。
2. 電子署名の適格証明書は、別紙 I に定める要求事項を超える強制的な要求事項に服するものとしてはならない。
3. 電子署名の適格証明書は、非義務的で付加的な特定の属性を含めることができる。その属性は、適格電子署名の相互運用性及び承認を害してはならない。
4. 電子署名の適格証明書が初期アクティブ化の後に破棄された場合、その破棄の時からその有効性が失われ、かつ、そのステータスは、いかなる態様においても、回復されない。
5. 以下の要件に従い、構成国は、電子署名の適格証明書の一時的な停止に関し、国内法令を定めることができる:
(a) 電子署名の適格証明書が一時的に停止された場合、当該証明書は、その停止の期間内、その有効性を喪失するものとする;
(b) 停止期間は、証明書データベースの中に明確に表示され、停止のステータスは、その

停止の期間内、証明書のステータスに関する情報を提供するサービスから確認できるものとする。

6. 欧州委員会は、実装法令により、電子署名の適格証明書のための技術標準の参照番号を定めることができる。電子署名の適格証明書がこれらの技術標準に適合する場合、別紙 I に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 29 条　適格電子署名作成機器の要求事項

1. 適格電子署名作成機器は、別紙 II に定める要求事項に適合するものとする。
2. 欧州委員会は、実装法令により、適格電子署名作成機器のための技術標準の参照番号を定めることができる。適格電子署名作成機器がこれらの技術標準に適合する場合、別紙 II に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 30 条　適格電子署名作成機器の認証

1. 適格電子署名作成機器の別紙 II に定める要求事項の遵守は、構成国から指定された適切な公的組織または民間組織によって認証される。
2. 構成国は、欧州委員会に対し、第 1 項に示す公的組織または民間組織の名称及び住所を通知する。欧州委員会は、構成国に対し、その情報を利用可能なものとする。
3. 第 1 項に示す認証は、以下のいずれかに基づく:

(a) 第 2 副項に従って作成されるリストの中に含まれる情報技術製品の安全性評価のための技術標準のいずれかに従って、安全性評価プロセスが実施されたこと;または

(b) それが同等な安全性レベルを用いるものである限り、かつ、第 1 項に示す公的組織または民間組織が、欧州委員会に対して当該作業を通知する限り、(a)に示すプロセス以外のプロセス。そのプロセスは、(a)に示す技術標準が存在しない場合、または、(a)に示す安全性評価プロセスが進行している場合に限り、これを用いることができる。

欧州委員会は、実装法令により、(a)に示す情報技術製品の安全性評価のための技術標準のリストを作成できる。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

4. 欧州委員会は、本条の第 1 項に示す指定された機関が適合すべき特別の基準を設けることに関し、第 47 条に従って委任される行為を採択する権限をもつ。

第 31 条　認証適格電子署名作成機器のリストの公示

1. 構成国は、欧州委員会に対し、不適切な遅滞なく、かつ、遅くとも、認証が実施された後 1 か月以内に、第 30 条第 1 項に示す組織によって認証された適格電子署名作成機器に関する情報を通知する。構成国は、欧州委員会に対し、不適切な遅滞なく、かつ、遅くとも、その認証が取り消された後 1 か月以内に、認証されなくなった電子署名作成機器に関する情

報も通知する。
2. 受領した情報に基づき、欧州委員会は、認証された適格電子署名作成機器のリストを作成し、公表し、かつ、維持管理する。
3. 欧州委員会は、実装法令により、第 1 項の目的のために適用可能なフォーマット及び手続を定める。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 32 条　適格電子署名の有効性の要求事項

1. 適格電子署名の有効性確認のためのプロセスは、以下を条件として、適格電子署名の有効性を確認する:
(a) その署名をサポートする証明書が、署名の時点において、別紙 I を遵守する電子署名のための適格証明書であったこと;
(b) 適格証明書が、適格信頼サービスプロバイダによって発行されたものであり、かつ、その署名の時点において、有効なものであったこと;
(c) 署名有効性確認データが、依拠者に対して提供されたデータに対応するものであること;
(d) 証明書の中で署名者を示すユニークなセットのデータが、依拠者に対し正確に提供されること;
(e) 署名の時点において仮名が使用された場合、仮名が使用されたことが、依拠者に対して明確に表示されること;
(f) その電子署名が、適格電子署名作成機器によって作成されたこと;
(g) 署名されたデータの完全性が損なわれていないこと;
(h) 署名の時点において、第 26 条に定める要求事項が遵守されたこと。
2. 適格電子署名の有効性確認のために使用されるシステムは、依拠者に対して正確な有効性確認結果を提供し、かつ、安全性と関連する問題を依拠者が検出できるものとする。
3. 欧州委員会は、実装法令により、適格電子署名の有効性確認のための技術標準の参照番号を定めることができる。適格電子署名の有効性確認がこれらの技術標準に適合する場合、第 1 項に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 33 条　適格電子署名の適格有効性確認サービス

1. 適格電子署名のための適格有効性確認サービスは、以下の適格信頼サービスプロバイダによってのみ、提供され得る:
(a) 第 32 条第 1 項を遵守する有効性確認を提供し;かつ
(b) 信頼性があり、正確であり、かつ、その適格有効性確認サービスのプロバイダの高度電子署名または高度電子シールを担う、自動的な手段による有効性確認プロセスの結果を依拠者が取得できるようにするプロバイダ。
2. 欧州委員会は、実装法令により、第 1 項に示す適格有効性確認サービスのための技術標準の参照番号を定めることができる。適格電子署名の有効性確認サービスがこれらの技

術標準に適合する場合、第 1 項に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 34 条　適格電子署名の適格保存サービス

1. 適格電子署名の適格保存サービスは、技術上の有効期間を超えて適格電子署名の信頼性を拡大することのできる手続及び技術を使用する適格信頼サービスプロバイダによってのみ提供され得る。
2. 欧州委員会は、実装法令により、適格電子署名の適格保存サービスのための技術標準の参照番号を定めることができる。適格電子署名の適格保存サービスのための準備がこれらの技術標準に適合する場合、第 1 項に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 5 節　電子シール

第 35 条　電子シールの法的効果

1. 電子シールは、それが電子的な方式によるものであること、または、それが適格電子シールの要求事項に適合しないことのみを理由として、法的効果及び訴訟手続における証拠としての許容性を否定してはならない。
2. 適格電子シールは、データの完全性の推定、及び、その適格電子シールが関係付けられるデータの原本の正確性の推定を享受する。
3. ある構成国内で発行された適格証明書に基づく適格電子シールは、他の全ての構成国において、適格電子シールとして承認される。

第 36 条　高度電子シールの要求事項

高度電子シールは、以下の要求事項に適合するものとする:

(a) そのシールの作成者とユニークに関連付けられるものであること;
(b) そのシールの作成者を識別できるものであること;
(c) そのシールの作成者が、その作成者のみの管理下で、高いレベルの機密性をもって、使用できる電子シール作成データを使用して作成されるものであり;かつ
(d) データ内のその後の変更が検出可能であるような方法で、関連データと関連付けられるものであること。

第 37 条　公的サービスにおける電子シール

1. 公的部門の組織によって、または、その代りに提供されるオンラインサービスを利用するために、高度電子シールを構成国が要求する場合、当該構成国は、高度電子シール、電子シールの適格証明書に基づく高度電子シール、及び、少なくとも、第 5 項に示す実装法令

に定めるフォーマットまたは使用方法による適格電子シールを承認する。
2. 公的部門の組織によって、または、その代りに提供されるオンラインサービスを利用するために、適格証明書に基づく高度電子シールを構成国が要求する場合、当該構成国は、適格証明書に基づく高度電子シール、及び、少なくとも、第 5 項に示す実装法令に定めるフォーマットまたは使用方法による適格電子シールを承認する。
3. 構成国は、公的部門の組織によって提供されるオンラインサービスにおける国境を越える使用について、適格電子シールよりも高い安全性レベルの電子シールを要求してはならない。
4. 欧州委員会は、実装法令により、高度電子シールのための技術標準の参照番号を定めることができる。高度電子シールがこれらの技術標準に適合する場合、本条第 1 項及び第 2 項並びに第 36 条に示す高度電子シールの要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。
5. 2015 年 9 月 18 日までに、かつ、既存の実務、技術標準及び欧州連合の法的行為を考慮に入れた上で、欧州委員会は、実装法令により、高度電子シールの参照フォーマットまたは代替的なフォーマットが使用される場合の参照手段を定めることができる。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 38 条　電子シールの適格証明書

1. 電子シールの適格証明書は、別紙 III に定める要求事項に適合するものとする。
2. 電子シールの適格証明書は、別紙 III に定める要求事項を超える強制的な要求事項に服するものとしてはならない。
3. 電子シールの適格証明書は、非義務的で付加的な特定の属性を含めることができる。その属性は、適格電子シールの相互運用性及び承認を害してはならない。
4. 電子シールの適格証明書が初期アクティブ化の後に破棄された場合、その破棄の時からその有効性が失われ、かつ、そのステータスは、いかなる態様においても、回復されない。
5. 以下の要件に従い、構成国は、電子シールの適格証明書の一時的な停止に関し、国内法令を定めることができる:
(a) 電子シールの適格証明書が一時的に停止された場合、当該証明書は、その停止の期間内、その有効性を喪失するものとする;
(b) 停止期間は、証明書データベースの中に明確に表示され、停止のステータスは、その停止の期間内、証明書のステータスに関する情報を提供するサービスから確認できるものとする。
6. 欧州委員会は、実装法令により、電子シールの適格証明書のための技術標準の参照番号を定めることができる。電子シールの適格証明書がこれらの技術標準に適合する場合、別紙 III に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 39 条　適格電子シール作成機器

1. 第 29 条は、適格電子シール作成機器の要求事項に関し、準用して適用される。
2. 第 30 条は、適格電子シール作成機器の認証に関し、準用して適用される。
3. 第 31 条は、認証された適格電子シール作成機器の公表に関し、準用して適用される。

第 40 条　適格電子シールの有効性確認及び保存

第 32 条、第 33 条及び第 34 条は、適格電子シールの有効性確認及び保存に関し、準用して適用される。

第 6 節　電子タイムスタンプ

第 41 条　電子タイムスタンプの法的効果

1. 電子タイムスタンプは、それが電子的な方式によるものであること、または、それが適格電子タイムスタンプの要求事項に適合しないことのみを理由として、法的効果及び訴訟手続における証拠としての許容性を否定してはならない。
2. 適格電子タイムスタンプは、それが表示する日付及び時刻の正確性の推定、並びに、その日付及び時刻が結びつけられるデータの完全性の推定を享受する。
3. ある構成国内で発行された適格証明書に基づく適格電子タイムスタンプは、他の全ての構成国において、適格電子タイムスタンプとして承認される。

第 42 条　適格電子タイムスタンプの要求事項

1. 適格電子タイムスタンプは、以下の要求事項に適合するものとする:
(a) 検出されずにデータが変更される可能性を合理的に排除するような方法で、日付及び時刻をデータに結び付けるものであること;
(b) 協定世界時と関係付けられる正確なタイムソースに基づくものであること;
(c) 適格信頼サービスプロバイダの高度電子署名を用いて署名され、もしくは、高度電子シールでシールされ、または、何らかの均等な手段によるものであること。
2. 欧州委員会は、実装法令により、日付及び時刻とデータとの結びつきのための技術標準並びに正確なタイムソースのための技術標準の参照番号を定めることができる。日付及び時刻とデータとの結びつき及び正確なタイムソースがこれらの技術標準に適合する場合、第 1 項に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 7 節　電子登録配達サービス

第 43 条　電子登録配達サービスの法的効果

1. 電子登録配達サービスを使用して送信及び受信されたデータは、それが電子的な方式によるものであること、または、それが適格電子タイムスタンプの要求事項に適合しないことのみを理由として、法的効果及び訴訟手続における証拠としての許容性を否定してはならない。
2. 電子登録配達サービスを使用して送信及び受信されたデータは、データの完全性、識別される送信者による当該データの送信、識別される受信者によるそのデータの受信、並びに、電子登録配達サービスによって表示された送信及び受信の日付及び時刻の正確性の推定を享受する。

第 44 条　適格電子登録配達サービスの要求事項

1. 電子登録配達サービスは、以下の要求事項に適合するものとする:
(a) 1 または複数の信頼サービスプロバイダによって提供されるものであること;
(b) 高いレベルの信頼性をもって、送信者の識別子を確保するものであること;
(c) そのデータの配達の前に、受信者の識別子を確保するものであること;
(d) 検出されずにデータが変更される可能性を合理的に排除するような方法で、適格信頼サービスプロバイダの高度電子署名を用いて署名され、もしくは、高度電子シールでシールされることにより、データの送信及び受信が防護されるものであること;
(e) データの送信または受信の目的のために必要となるデータの変更が、そのデータの送信者または受診者に対して明確に表示されるものであること;
(f) データの送信、受信、及び、データの変更の日付及び時刻が、適格電子タイムスタンプによって表示されるものであること;
　複数の適格信頼サービスプロバイダ間でデータが送信される場合、その全ての適格信頼サービスプロバイダに対し、(a)ないし(f)の要求事項が適用される。
2. 欧州委員会は、実装法令により、データの送信及び受信の目的のための技術標準の参照番号を定めることができる。データの送信及び受信のための処理がこれらの技術標準に適合する場合、第 1 項に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 8 節　Web サイト確認

第 45 条　適格 Web サイト確認証明書の要求事項

1. 適格 Web サイト確認証明書は、別紙 IV に定める要求事項に適合するものとする。
2. 欧州委員会は、実装法令により、適格 Web サイト確認証明書のための技術標準の参照番号を定めることができる。適格 Web サイト確認証明書がこれらの技術標準に適合する場合、

別紙 IV に定める要求事項の遵守が推定される。これらの実装法令は、第 48 条第 2 項による審議手続に従い、採択される。

第 4 章　電子文書

第 46 条　電子文書の法的効果

電子文書は、それが電子的な方式によるものであることのみを理由として、法的効果及び訴訟手続における証拠としての許容性を否定してはならない。

第 5 章　権限の委任及び実装条項

第 47 条　委任の実施

1. 本条に定める要件に従い、欧州委員会に対し、委任された行為を採択する権限が与えられる。
2. 第 30 条第 4 項に示す委任された行為を採択する権限は、2014 年 9 月 17 日からの不確定期限により、欧州委員会に対して与えられる。
3. 欧州議会または理事会は、いつでも、第 30 条第 4 項に示す委任を取消すことができる。取消しの決定は、当該決定の中で指定された権限の委任を終了させる。その取消しは、EU 官報上でその決定が公示された翌日、または、遅くとも、その決定の中で指定された日に発効する。その決定は、既に発効している委任された行為の有効性を害さない。
4. 欧州委員会が委任された行為を採択する場合、欧州委員会は、直ちに、欧州議会及び理事会に対し、同時に通知する。
5. 第 30 条第 4 項により採択される委任された行為は、欧州議会及び理事会に対する当該行為の通知から 2 か月以内に欧州議会または理事会のいずれからも異議が表明されない場合、または、当該期限が満了する前に、欧州議会及び理事会の両者が、欧州委員会に対し、異議を述べないことを連絡した場合においてのみ、発効する。この期限は、欧州議会または理事会の発意により、これを 2 か月まで延長できる。

第 48 条　委員会の手続

1. 欧州委員会は、委員会によって補佐される。この委員会は、規則(EU) No 182/2011 の意味における委員会である。
2. 本項に対する参照が行われる場合、規則(EU) No 182/2011 の第 5 条が適用される。

第 6 章　最終条項

第 49 条　見直し

1. 欧州委員会は、この規則の適用を見直し、かつ、欧州議会及び理事会に対し、遅くとも 2020 年 7 月 1 日までに、報告する。欧州委員会は、この規則の適用によって得られた経験、並びに、技術的な発展、市場の発展及び法的な発展を考慮に入れた上で、とりわけ、この規則の適用範囲、または、第 6 条、第 7 条(f)並びに第 34 条、第 43 条、第 44 条及び第 45 条を含め、この規則の特定の条項の適用範囲を修正することが適切であるか否かを評価する。
2. 第 1 項に示す報告書は、それが適切なときは、立法提案を添付するものとする。
3. 加えて、欧州委員会は、欧州議会及び理事会に対し、第 1 項に示す報告の後、4 年毎に、この規則の目標の到達に向けた進捗状況に関する報告書を提出する。

第 50 条　廃止

1. 指令 1999/93/EC は、2016 年 7 月 1 日をもって廃止される。
2. 廃止される指令に対する参照は、この規則に対する参照として解釈される。

第 51 条　移行措置

1. その適格性が、指令 1999/93/EC の第 3 条第 4 項に従って決定された電子署名作成機器は、この規則に基づく適格電子署名作成機器とみなされる。
2. 指令 1999/93/EC に基づき自然人に対して発行された適格証明書は、この指令に基づく電子署名の適格証明書とみなされる。
3. 指令 1999/93/EC に基づき適格証明書を発行する認証サービスプロバイダは、可及的速やかに、かつ、遅くとも、2017 年 7 月 1 日までに、監督機関に対し、適格性評価報告書を提出する。その適格性評価報告書の提出及び監督機関によるその評価の完了までは、当該認証サービスプロバイダは、この規則に基づく適格信頼サービスプロバイダとみなされる。
4. 指令 1999/93/EC に基づき適格証明書を発行する認証サービスプロバイダが、第 3 項に示す期限内に、監督機関に対して適格性評価報告書を提出しない場合、当該認証サービスプロバイダは、2017 年 7 月 2 日以降、この規則に基づく適格信頼サービスプロバイダとみなされない。

第 52 条　発効

1. この規則は、EU 官報上で公示された翌日から 20 日目に発効する。
2. 以下の条項を除き、この規則は、2016 年 7 月 1 日から適用される:

(a) 第 8 条第 3 項、第 9 条第 5 項、第 12 条第 2 項ないし第 9 項、第 17 条第 8 項、第 19 条第 4 項、第 20 条第 4 項、第 21 条第 4 項、第 22 条第 5 項、第 23 条第 3 項、第 24 条第 5 項、第 27 条第 4 項及び第 5 項、第 28 条第 6 項、第 29 条第 2 項、第 30 条第

3 項及び第 4 項、第 31 条第 3 項、第 32 条第 3 項、第 33 条第 3 項、第 34 条第 2 項、第 37 条第 4 項及び第 5 項、第 38 条第 6 項、第 42 条第 2 項、第 44 条第 2 項、第 45 条第 2 項並びに第 47 条及び第 48 条は、2014 年 9 月 17 日から適用される。

(b) 第 7 条、第 8 条第 1 項及び第 2 項、第 9 条、第 10 条、第 11 条並びに第 12 条第 1 項は、第 8 条第 3 項及び第 12 条第 8 項に示す実装法令の適用の日から適用される。

(c) 第 6 条は、第 8 条第 3 項及び第 12 条第 8 項に示す実装法令の適用の日の 3 年後から適用される。

3. 通知された電子識別スキームが、本条第 2 項(c)に示す日の前に、第 9 条により欧州委員会によって公示されるリストの中に含められる場合、第 6 条による当該スキームに基づく電子識別手段の承認は、当該スキームの公示から遅くとも 12 か月以内に、かつ、本条の第 2 項(c)に示す日以降に、行われる。

4. 本条の第 2 項(c)に拘らず、構成国は、別の構成国から第 9 条第 1 項により通知された電子識別スキームに基づく電子識別手段が前者の構成国内において、第 8 条第 3 項及び第 12 条第 8 項に示す実装法令の日からのものとして承認されることを決定し得る。関係する構成国は、欧州委員会に対し、そのことを連絡する。欧州委員会は、その情報を公表する。

この規則は、その全部について拘束力があり、かつ、全ての構成国において直接に適用される。

2014 年 7 月 23 日にブリュッセルにおいて行われた。

欧州議会として	理事会として
議長　M. Schulz	議長　S. Gozi

別紙 I

電子署名の適格証明書の要求事項

電子署名の適格証明書は、以下の事項を含めるものとする:

(a) 少なくとも自動的な処理に適した方式により、その証明書が電子署名のための適格証明書として発効されたことの表示;

(b) 少なくとも、当該プロバイダが設立されている構成国及び以下の事項を含め、適格証明書を発行する適格信頼サービスプロバイダを紛れなく示すデータのセット:
   - 法人について:その名前、及び、それが適切なときは、公式記録に示されている登録番号、
   - 自然人について:その者の氏名;

(c) 少なくとも、署名者の氏名または仮名;仮名が使用される場合、そのことが明確に表示される;

(d) 電子署名作成データと対応する電子署名有効性確認データ;

(e) 証明書の有効期限の始期及び終期の詳細;

(f) 証明書識別コード、それは、適格信頼サービスプロバイダにとってユニークなものでなければならない;

(g) 発行者である適格信頼サービスプロバイダの高度電子署名または高度電子シール;

(h) (g)に示す高度電子署名または高度電子シールをサポートする証明書を無料で使用できる場所の所在地;

(i) 適格証明書の有効性ステータスに関して問い合わせるために使用できるサービスの所在地;

(j) 電子署名有効性確認データと関連する電子署名作成データが適格電子署名作成機器の中にある場合、少なくとも自動的な処理に適した方式により、その機器の適切な表示。

別紙 II

適格電子署名作成機器の要求事項

1. 適格電子署名作成機器は、適切な技術上及び手続上の措置により、少なくとも、以下を確保するものとする:
   (a) 電子署名作成のために使用される電子署名作成データの機密性が合理的に保証されること;
   (b) 電子署名作成のために使用される電子署名作成データが、実際に、1 度だけ発生させることができるものであること;
   (c) 電子署名作成のために使用される電子署名作成データが、合理的な保証のあるものとして、配布され得ないものであり、かつ、その電子署名が、現在利用可能な技術を使用する偽造に対し、信頼性のあるものとして、保護されるものであること;
   (d) 電子署名作成のために使用される電子署名作成データが、第三者による使用に対し、信頼性のあるものとして、適法な署名者によって保護され得るものであること。
2. 適格電子署名作成機器は、署名されるデータを変更してはならず、または、署名の前に、署名者に対してそのデータが表示されることを妨げてはならない。
3. 署名者の代わりに行われる電子署名作成データの生成または維持管理は、適格信頼サービスプロバイダによってのみ、これを行うことができる。
4. 1 の(d)を妨げることなく、署名者の代わりに適格信頼サービスプロバイダが維持管理する電子署名作成データは、以下の要求事項に適合する場合に限り、バックアップの目的のためにのみ、電子署名作成データを複製できる:
   (a) 複製されるデータセットの安全性は、原本であるデータセットと同じレベルのものでなければならない;
   (b) 複製されるデータセットの数は、サービスの継続性を確保するために必要なミニマムの数を超えることができない。

別紙 III

電子シールの適格証明書の要求事項

電子シールの適格証明書は、以下のものを含めるものとする:

(a) 少なくとも自動的な処理に適した方式により、その証明書が電子シールのための適格証明書として発効されたことの表示;
(b) 少なくとも、当該プロバイダが設立されている構成国及び以下の事項を含め、適格証明書を発行する適格信頼サービスプロバイダを紛れなく示すデータのセット:
  － 法人について:その名前、及び、それが適切なときは、公式記録に示されている登録番号、
  － 自然人について:その者の氏名;
(c) 少なくとも、シール作成者の名前、及び、それが適切なときは、公式記録に示されている登録番号;
(d) 電子シール作成データと対応する電子シール有効性確認データ;
(e) 証明書の有効期限の始期及び終期の詳細;
(f) 証明書識別コード、それは、適格信頼サービスプロバイダにとってユニークなものでなければならない;
(g) 発行者である適格信頼サービスプロバイダの高度電子署名または高度電子シール;
(h) (g)に示す高度電子署名または高度電子シールをサポートする証明書を無料で使用できる場所の所在地;
(i) 適格証明書の有効性ステータスに関して問い合わせるために使用できるサービスの所在地;
(j) 電子シール有効性確認データと関連する電子シール作成データが適格電子シール作成機器の中にある場合、少なくとも自動的な処理に適した方式により、その機器の適切な表示。

別紙 IV

適格 Web サイト確認証明書の要求事項

適格 Web サイト確認証明書は、以下のものを含めるものとする:

(a) 少なくとも自動的な処理に適した方式により、その証明書が適格 Web サイト確認証明書のための適格証明書として発効されたことの表示;

(b) 少なくとも、当該プロバイダが設立されている構成国及び以下の事項を含め、適格証明書を発行する適格信頼サービスプロバイダを紛れなく示すデータのセット:
- 法人について:その名前、及び、それが適切なときは、公式記録に示されている登録番号、
- 自然人について:その者の氏名;

(c) 自然人について:少なくとも、その証明書が発行される者の氏名または仮名。仮名が使用される場合、そのことが明確に表示される
法人について:少なくとも、その証明書が発行される法人の名前、及び、それが適切なときは、公式記録に示されている登録番号;

(d) その証明書が発行される自然人または法人の少なくとも市及び国を含む住所の要素、並びに、それが適用可能なとしては、公式記録に示されているとおりに;

(e) その証明書が発行される自然人または法人によって運営されているドメイン名;

(f) 証明書の有効期限の始期及び終期の詳細;

(g) 証明書識別コード、それは、適格信頼サービスプロバイダにとってユニークなものでなければならない;

(h) 発行者である適格信頼サービスプロバイダの高度電子署名または高度電子シール;

(i) (h)に示す高度電子署名または高度電子シールをサポートする証明書を無料で使用できる場所の所在地;

(j) 適格証明書の有効性ステータスに関して問い合わせるために使用できる証明書有効性ステータスサービスの所在地。