委員会実装規則 (EU) 2015/1502

[参考訳]

2017 年 10 月 14 日
明治大学法学部教授
夏 井 高 人

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market（OJ L 235, 9.9.2015, p.7-20）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:32015R1502&from=EN
[2017 年 10 月 6 日確認]

この委員会実装規則 (EU) 2015/1502（以下「実装規則 2015/1502」という。）は、電子識別規則(EU) No 910/2014 に基づいて欧州委員会が採択した実装法令（施行細則）の 1 つである。

実装規則 2015/1502 は、規則(EU) No 910/2014 第 8 条第 3 項による電子識別手段の信頼レベルを定めるものである。

実装規則 2015/1502 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、あくまでも実装規則 2015/1502 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。

実装規則 2015/1502 の内容の詳細は、条文によってではなく、別紙の中で定められている。それらの別紙に定める事項の中で、日本国の類似の業務においても全般的に比較的よく遵守されているのは、2.4.6.の技術上の管理策の部分のみと言ってよい。それ以外の部分は、日本特有の歴史的・風土的要因によるものかどうか、比較的曖昧な運用となっていることが決して珍しくない。

そのような状況が醸成された主要な要因の 1 つとして、初等教育から高等教育まで貫かれている理系と文系の区別という粗雑な促成栽培的教育システムにあることは、言うまでもないことである。このシステムは、戦時体制を想定するものであるから、日本国の教育制度の根本思想は、まだ第二次世界大戦中の発想のままであるということができる。

しかし、現代の社会において真に求められているのは、理系・文系の区別を完全に無視し、全ての分野に関して十分な知識と理解力があることを必須の前提とした上で、それぞれの専門分野をもつような人材である。とりわけ、情報処理に関する知識・技能は、分野を問わず、必須のものである。

（この参考訳を作成する際に考慮した事項）

「authoritative source」は、本人確認のために使用される様々な証明資料の情報源のことを意味する（別紙の定義条項参照）。この参考訳においては、「authoritative source」を「確認情報源」と訳すことにした。

「authentication factor」は、ある識別子と本人とを結びつける要素のことを意味する（別紙の定義条項参照）。この参考訳においては、「authentication factor」を「確認要素」と訳すことにした。

「enrolment」は、本人確認等の手続を経て個人識別をするための識別子を生成し、登録する手続の全体を指すものであり、具体的なデータの記録保存または送信に該当する「登録（registration）」よりも広い概念である。

「登録（registration）」との区別が曖昧になるという難があるけれども、この参考訳においては、「enrolment」を、便宜、「登録」と訳すことにした。

以上のほかは、電子識別規則(EU) No 910/2014 の参考訳（法と情報雑誌 2 巻 10 号 147～196 頁）で述べたところと同じである。

＊＊＊

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に関する欧州議会及び理事会の規則 (EU) No 910/2014 の第 8 条第 3 項による電子識別手段の信頼レベルのためのミニマムの技術仕様及び手続を定める 2015 年 9 月 8 日の委員会実装規則 (EU) 2015/1502

欧州委員会は、
欧州連合の機能に関する条約に鑑み、
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[1]、並びに、とりわけ、その第 8 第 3 項に鑑み、
以下のとおりであるので、この規則を採択する。

(1) 規則(EU) No 910/2014 第 8 条は、第 9 条第 1 項により通知される電子識別スキームが、当該スキームに基づいて発行される電子識別手段のための低、十分及び高の信頼レベルを指示することを要する旨を定めている。
(2) 信頼レベルの詳細についての共通理解を確保するため、及び、規則(EU) No 910/2014 第 12 条第 4 項(b)に定める、通知された電子識別スキームの国内信頼レベルと第 8 条に基づく信頼レベルとのマッピングを確保するために、ミニマムの技術仕様、技術標準及び手続を定めることが重要である。
(3) 国際規格 ISO/IEC 29115 は、電子識別手段のドメインにおいて利用可能な基本原則である国際規格となるものとして、この実装法令に定める仕様及び手続を考慮に入れた。しかしながら、規則(EU) No 910/2014 の内容は、とりわけ、同一性の証明及び検証の要求事項に関し、並びに、構成国の同一性識別方法と、同じ目的による EU の既存のツールとの間の相違を考慮に入れる方法に関し、同国際規格とは異なっている。それゆえ、別紙は、国際規格に基づいて構築されているとはいえ、ISO/IEC 29115 の特定のコンテントへの参照を行ってはならない。
(4) この規則は、条件及び概念を指示するために使用される定義の中にも反映される最も適切なアプローチの結果に基づいて開発された。それは、電子識別手段の保証レベルに関し、規則(EU) No 910/2014 の目的を考慮に入れている。それゆえ、それによって開発された仕様を含め、大規模パイロット STORK 及び ISO/IEC 29115 の中にある定義及び概念は、この実装法令に定める仕様及び手続を確立する際、最大限考慮に入れなければならない。
(5) 同一性の証拠の側面が検証される必要のある過程の相違により、確認情報源は、登録、文書、就中、組織といったような多種多様な形態をとり得る。確認情報源は、同じ過程においてさえ、様々な異なる構成国の中において異なったものであり得る。

[1] OJ L 257, 28.8.2014, p.73.

(6) 同一性の証明及び検証の要求事項は、必要となる信頼を確立するために、十分な高さを確保しつつ、異なるシステム及び実務を考慮に入れなければならない。それゆえ、電子識別手段の発行以外の目的のために従前使用された手続の承認は、その手続が、対応する保証レベルにおいて予定される要求事項を満たすものであることの確認を条件として行われなければならない。
(7) 秘密の共有、物理装置及び身体属性のような一定の確認要素は、通常、うまく働く。しかしながら、確認プロセスの安全性を向上させるため、特に異なる要素カテゴリから得られる、より多数の確認要素の使用が奨励される。
(8) この規則は、法人の代表の権利を害してはならない。しかしながら、別紙は、電子識別手段と自然人及び法人との結合のための要求事項を定めるものとしなければならない。
(9) 承認された手法がうまく働くこと、そして、IS/IEC 27000 及び ISO/IEC 20000 シリーズのような規格の中に置かれた基本原則が適用されることが重要性をもつので、情報セキュリティ及びサービスマネジメントシステムの重要性が認識されなければならない。
(10) 構成国における保証レベルと関連するグッドプラクティスが考慮に入れられなければならない。
(11) 国際規格に基づく IT セキュリティ認証は、この実装法令の要求事項への製品の遵守を検証するための重要なツールの 1 つである。
(12) この規則に定める措置は、規則(EU) No 910/2014 第 48 条に示す委員会の意見に従うものである。

第 1 条

1. 通知された電子識別スキームの基づき発行される電子識別手段のための低、十分及び高の保証レベルは、別紙に定める仕様及び手続を参照して決定される。
2. 別紙に定める仕様及び手続は、以下の要素の信頼性及び品質を決定することにより、通知された電子識別スキームに基づいて発行される電子識別手段の保証レベルを指示するために使用される:
(a) 規則(EU) No 910/2014 第 8 条第 3 項(a)により、この指令の別紙の 2.1 節に定める登録;
(b) 規則(EU) No 910/2014 第 8 条第 3 項(b)及び(f)により、この指令の別紙の 2.2 節に定める電子識別手段の管理;
(c) 規則(EU) No 910/2014 第 8 条第 3 項(c)により、この指令の別紙の 2.3 節に定める確認;
(d) 規則(EU) No 910/2014 第 8 条第 3 項(d)及び(e)により、この指令の別紙の 2.4 節に定める管理及び組織。
3. 通知された電子識別スキームの基づき発行される電子識別手段が、より高い保証レベルに列挙されている要求事項に適合する場合、その電子識別手段は、より低い保証レベルと均等な要求事項を満たすものと推定される。

4. 別紙の関連する部分の中で別異に示されていない限り、主張された保証レベルとの適合のために、その通知された電子識別スキームの基づき発行される電子識別手段の特定の保証レベルのために別紙の中に列挙されている全ての要素に適合するものとする。

第 2 条

この規則は、EU 官報上で公示された翌日から 20 日目の日に発効する。

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。

2015 年 9 月 8 日にブリュッセルにおいて行われた。

欧州委員会として

議長　Jean-Claude Juncker

別　紙

通知された電子識別スキームの基づき発行される電子識別手段のための低、十分及び高の保証レベルは、別紙に定める仕様及び手続

1. 適用可能な定義

この別紙の目的のために、以下の定義が適用される:

(1) 「確認情報源（authoritative source）」とは、その形態の別を問わず、同一性の証明のために使用することのできる正確なデータ、情報及びまたは証拠を提供するために依拠することのできる全ての情報源を意味し;

(2) 「確認要素（authentication factor）」とは、個人と結びつけられているものとして確認される要素であって、以下のカテゴリの範囲内にあるもののことを意味する:
   (a) 「所持に基づく確認要素（possession-based authentication factor）」とは、法主体が、それを所持していることを示すことが求められる要素のことを意味し;
   (b) 「知識に基づく確認要素（knowledge-based authentication factor）」とは、法主体が、その知識を示すことが求められる要素のことを意味し;
   (c) 「固有の確認要素（inherent authentication factor）」とは、自然人の身体属性を基礎とするものであり、かつ、法主体が、その身体属性をもつことを示すことが求められる確認要素のことを意味し;

(3) 「動的確認（dynamic authentication）」とは、法主体が識別データを管理または所持していることの電子的な証明をオンデマンドで作成する手段を提供するための暗号またはその他の技術を用いる電子的な処理であり、かつ、法主体と、法主体の同一性を検証するシステムとの間の個々の確認を変化させるもののことを意味し;

(4) 「情報セキュリティマネジメントシステム（information security management system）」とは、情報セキュリティと関連する受容可能なレベルのリスクを管理するために設計された一群の処理及び手順のことを意味する。

2. 技術仕様及び手続

この別紙に概要を示す技術仕様及び手続の要素は、規則(EU) No 910/2014 第 8 条の要求事項及び基準が、電子識別スキームに基づいて発行される電子識別手段についてどのように適用されるかを決定するために使用される。

2.1. 登録（Enrolment）

2.1.1. 申請及び登録（Registration）

保証レベル	必要な要素
低	1.　申請者が、電子識別手段の使用と関連する契約条件及び要件に留意

	することを確保する。 2. 申請者が、電子識別手段と関連する推奨される安全性警告に留意することを確保する。 3. 同一性の証明及び検証のために必要な関連同一性識別データを収集する。
十分	低のレベルと同じ
高	低のレベルと同じ

2.1.2. 同一性の証明及び検証（自然人）

保証レベル	必要な要素
低	1. その者が、その電子識別手段の申請が行われる構成国によって承認され、かつ、主張された同一性を示す証拠を所持するものと推定され得ること。 2. その証拠が、真正なものと推定され、または、確認情報源によって存在するものと推定され得るものであり、かつ、その証拠が一応有効であると見えること。 3. 主張された同一性が存在することが確認情報源によって認識され、かつ、その同一性を主張する者が単一かつ同一であると推定され得ること。
十分	低のレベルであることに加え、1 ないし 4 に列挙する代替要素の 1 つに該当しなければならない: 1. その者が、その電子識別手段の申請が行われる構成国によって承認され、かつ、主張された同一性を示す証拠を所持することが検証され、 かつ、 その証拠が、真正なものであることを判定するために点検され;もしくは、確認情報源により、存在し、かつ、実在する個人と関係するものであると認識され、 かつ、 例えば、紛失し、盗難され、停止され、破棄され、または、無効な証拠のリスクを考慮に入れた上で、その者の同一性が主張された同一性ではないというリスクをミニマムなものとするための措置が講じられたこと; または、 2. その文書が発行された構成国における登録手続の中で身分証明の文書が提出され、かつ、その文書がそれを提出する者と関連するものであるように見え、 かつ、 例えば、紛失し、盗難され、停止され、破棄され、または、無効な証拠のリスクを考慮に入れた上で、その者の同一性が主張された同一性ではないというリスクをミニマムなものとするための措置が講じられたこと;

	または、 3. 電子識別手段の発行以外の目的のために同じ構成国内の公的組織または民間組織によって従前使用された手続が、十分のレベルの保証のための 2.1.2 節に定めるものと均等な保証を定めている場合、欧州議会及び理事会の規則(EC) No 765/2008[1]の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、そのような均等な評価が確認されている限り、その登録について職責を負う機関が、それらの従前の手続を繰り返して行う必要がないこと; または、 4. 十分または高の保証レベルをもち、かつ、個人識別データの改変のリスクを考慮に入れた上で、有効な通知された電子識別手段に基づいて電子識別手段が発行されている場合、同一性の証明及び検証のプロセスを繰り返すことが要求されないこと。通知されていない電子識別手段に基づくものとしてその電子識別手段が提供される場合、規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、十分または高の信頼レベルが確認されなければならないこと。
高	1 または 2 のいずれかの要求事項に適合しなければならない: 1. 十分のレベルであることに加え、(a)ないし(c)に列挙する代替要素の 1 つに該当しなければならない: (a) その者が、その電子識別手段の申請が行われる構成国によって承認され、かつ、主張された同一性を示す写真または生体要素による同一性識別の証拠を所持することが検証された場合、その証拠が、確認情報源によって有効であることを判定するために点検され、 かつ、 申請者が、確認情報源を用いる個人の 1 または複数の身体的特徴との比較により、主張された同一性のあるものとして識別されること; または、 (b) 電子識別手段の発行以外の目的のために同じ構成国内の公的組織または民間組織によって従前使用された手続が、高のレベルの保証のための 2.1.2 節に定めるものと均等な保証を定めており、そして、欧州議会及び理事会の規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関によってそのような均等な評価が確認されている限り、その登録について職責を負う機関が、それらの従前の手続を繰り返して行う必要がなく、 かつ、

[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）

	従前の手続がなお有効であるとの結論を示すための手立てが講じられていること; または、 (c) 高の保証レベルをもち、かつ、個人識別データの改変のリスクを考慮に入れた上で、有効な通知された電子識別手段に基づいて電子識別手段が発行されている場合、同一性の証明及び検証のプロセスを繰り返すことが要求されないこと。通知されていない電子識別手段に基づくものとしてその電子識別手段が提供される場合、規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、は高の信頼レベルが確認されなければならず、 かつ、 この従前の通知された電子識別手段の発行手続がなお有効であるとの結論を示すための手立てが講じられていること。 または、 2. 申請者が、写真または生体要素による同一性識別の証拠を提出しない場合、そのような承認された写真または生体要素による同一性識別の証拠を収集するために、登録の職責を負う組織の構成国内において、国内レベルで使用される全く同じ手続が適用されること。

2.1.3. 同一性の証明及び検証（法人）

保証レベル	必要な要素
低	1. 法人の主張された同一性が、その電子識別手段の申請が行われる構成国によって承認された証拠に基づいて示されること。 2. 確認情報源の中に法人を含めることが任意であり、かつ、その法人とその確認情報源との間の手続準則によって規律されるものである場合、その証拠が、一応有効なものであるように見え、かつ、真正なものと推定され、または、その確認情報源によって存在するものと推定され得るものであること。 3. その法人が、確認情報源によって、当該法人として活動することが妨げられるような状態にあるとは認識されていないこと。
十分	低のレベルであることに加え、1 ないし 3 に列挙する代替要素の 1 つに該当しなければならない: 1. その法人の名称、法形式及び（適用可能なときは）その登録番号を含め、法人の主張された同一性が、その電子識別手段の申請が行われる構成国によって承認された証拠に基づいて示され、 かつ、 確認情報源の中に法人を含めることがその分野において業務遂行するためにその法人に対して要求される場合、その証拠が、真正なものであ

	ることを判定するために点検され、もしくは、確認情報源により、存在するものであると認識され、 かつ、 例えば、紛失し、盗難され、停止され、破棄され、または、無効な証拠のリスクを考慮に入れた上で、その法人の同一性が主張された同一性ではないというリスクをミニマムなものとするための措置が講じられたこと; または、 2. 電子識別手段の発行以外の目的のために同じ構成国内の公的組織または民間組織によって従前使用された手続が、十分のレベルの保証のための 2.1.3 節に定めるものと均等な保証を定めている場合、欧州議会及び理事会の規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、そのような均等な評価が確認されている限り、その登録について職責を負う機関が、それらの従前の手続を繰り返して行う必要がないこと; または、 3. 十分または高の保証レベルをもち、有効な通知された電子識別手段に基づいて電子識別手段が発行されている場合、同一性の証明及び検証のプロセスを繰り返すことが要求されないこと。通知されていない電子識別手段に基づくものとしてその電子識別手段が提供される場合、規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、十分または高の信頼レベルが確認されなければならないこと。
高	十分のレベルであることに加え、1 ないし 3 に列挙する代替要素の 1 つに該当しなければならない: 1. その法人の名称、法形式及び国内において使用され、その法人を示す少なくとも 1 つのユニークな識別子を含め、法人の主張された同一性が、その電子識別手段の申請が行われる構成国によって承認された証拠に基づいて示され、 かつ、 その証拠が、確認情報源によって有効であることを判定するために点検されること; または、 2. 電子識別手段の発行以外の目的のために同じ構成国内の公的組織または民間組織によって従前使用された手続が、高のレベルの保証のための 2.1.3 節に定めるものと均等な保証を定めている場合、欧州議会及び理事会の規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、そのような均等な評価が確認されている限り、その登録について職責を負う機関が、それらの従前の手続を繰り返して行う必要がなく、 かつ、

	従前の手続がなお有効であるとの結論を示すための手立てが講じられていること; または、 3. 高の保証レベルをもち、有効な通知された電子識別手段に基づいて電子識別手段が発行されている場合、同一性の証明及び検証のプロセスを繰り返すことが要求されないこと。通知されていない電子識別手段に基づくものとしてその電子識別手段が提供される場合、規則(EC) No 765/2008 の第 2 条(13)に示す適合性評価機関またはそれと均等な組織によって、高の信頼レベルが確認されなければならず、 かつ、 この従前の通知された電子識別手段の発行手続がなお有効であるとの結論を示すための手立てが講じられていること。

2.1.4. 自然人の電子識別手段と法人の電子識別手段の結びつき

それが適用可能なときは、自然人の電子識別手段と法人の電子識別手段との間の結びつき(「結びつき」)について、以下の要件が適用される:

(1) 結びつきの停止及びまたは破棄が可能であること。結びつきのライフサイクル(例:アクティブ化、停止、更新、破棄)は、国内で承認された手続に従って管理運用される。

(2) その電子識別手段が法人の電子識別手段と結びつけられている自然人が、国内で承認された手続に基づき、その結びつけの実施を他の自然人に委任することができること。ただし、委任を受けた自然人は、説明責任を負うものとする。

(3) 結びつけが、以下の方法で行われること:

保証レベル	必要な要素
低	1. 法人の代わりに行動する自然人の同一性の証明が、低のレベルまたはそれ以上のレベルで行われたことが検証されること。 2. その結びつけが国内で承認された手続に基づいて確立されたこと。 3. その自然人が、確認情報源によって、当該法人の代わりに活動することが妨げられるような状態にあるとは認識されていないこと。
十分	低のレベルの 3 に加え: 1. その法人の代わりに行動する自然人の同一性の証明が、十分のレベルまたは高のレベルで行われたことが検証されること。 2. その結びつけが国内で承認された手続に基づいて確立され、それは、確認情報源の中にある結びつきの登録に帰結するものであること。 3. その結びつきが確認情報源からの情報に基づいて検証されること。
高	低のレベルの 3 及び十分のレベルの 3 に加え: 1. その法人の代わりに行動する自然人の同一性の証明が、高のレベルまたは高のレベルで行われたことが検証されること。 2. その結びつきが、国内で使用されるその法人を示すユニークな識別子

	に基づいて検証されること;かつ、確認情報源からのその自然人をユニークに示す情報に基づいて検証されること。

2.2. 電子識別手段の運用管理

2.2.1. 電子識別手段の特徴及び設計

保証レベル	必要な要素
低	1. その電子識別手段が、少なくとも、1 つの確認要素を用いるものであること。 2. その電子識別手段が、発行者に所属する者が管理または所持の下においてのみ使用される点検のための合理的な手立てを発行者が講ずるために設計されるものであること。
十分	1. その電子識別手段が、少なくとも、異なるカテゴリに属する 2 つの確認要素を用いるものであること。 2. その電子識別手段が、発行者に所属する者が管理または所持の下においてのみ使用されるとの推定を受けるために設計されるものであること。
高	十分のレベルに加え: 1. その電子識別手段が、複製及び改竄に対し、並びに、高度の攻撃力をもつ攻撃者に対し、防護されているものであること。 2. その電子識別手段が、その発行者に所属する者によって、第三者の使用に対し、信頼性のあるものとして防護され得るようにするために設計されるものであること。

2.2.2. 発行、配達及びアクティブ化

保証レベル	必要な要素
低	発行の後、その電子識別手段が、予定された者に対してのみ到達すると推定され得る仕組みを介して配達されること。
十分	発行の後、その電子識別手段が、発行者に所属する者の所持にのみ入るものとして配達されると推定され得る仕組みを介して配達されること。
高	アクティブ化のプロセスが、発行者に所属する者の所持にのみ入るものとしてその電子識別手段が配達されたことを検証するものであること。

2.2.3. 停止、破棄及び再アクティブ化

保証レベル	必要な要素
低	1. その電子識別手段が、適時かつ効果的な方法により停止及びまたは廃棄され得ること。 2. 無権限の停止、廃棄及びまたは再アクティブ化を防止するための手段

	が存在すること。 3. 停止または廃棄の前に確立されたのと同じ保証の要求事項に適合し続けている場合においてのみ、再アクティブ化が行われること。
十分	低のレベルと同じ
高	低のレベルと同じ

2.2.4. 更新及び交換

保証レベル	必要な要素
低	個人識別データの改変のリスクを考慮に入れた上で、更新または交換が、当初の同一性の証明及び検証と同じ保証の要求事項に適合するためであること、または、同等またはより高い保証レベルの有効な電子識別手段に基づくものであること。
十分	低のレベルと同じ
高	低のレベルに加え: 更新または交換が有効な電子識別手段に基づくものである場合、同一性識別データが、確認情報源を用いて検証されること。

2.3. 確認

この節は、確認メカニズムの使用と関係する脅威に焦点を当て、各保証レベルのための要求事項を列挙する。この節において、管理は、所与のレベルにおけるリスクに見合うものとして理解されるものとする。

2.3.1. 確認メカニズム

以下の表は、確認メカニズムに関し、保証レベル毎の要求事項を定める。それを通じて、自然人または法人は、依拠者に対し、その同一性を確認するための電子識別手段を使用する。

保証レベル	必要な要素
低	1. 個人識別データの公開が、その電子識別手段及びその有効性の信頼性のある検証の後に行われること。 2. 個人識別データが確認メカニズムの一部分として記録保存される場合、オフラインの解析の場合を含め、その情報が、総膣に対して保護され、かつ、漏洩に対して保護されるために、安全なものとすること。 3. 強化された基礎的な攻撃力をもつ攻撃者による通信の推測、傍受、再現または不正操作のような活動が確認メカニズムを破壊し得るようなことが高い確率で発生しないようにするため、その確認メカニズムが、電子識別手段の検証のためのセキュリティ管理を実装すること。

十分	低のレベルに加え: 1. 個人識別データの公開が、動的確認により、その電子識別手段及びその有効性の信頼性のある検証の後に行われること。 2. 中程度の攻撃力をもつ攻撃者による通信の推測、傍受、再現または不正操作のような活動が確認メカニズムを破壊し得るようなことが高い確率で発生しないようにするため、その確認メカニズムが、電子識別手段の検証のためのセキュリティ管理を実装すること。
高	十分のレベルに加え: 高度の攻撃力をもつ攻撃者による通信の推測、傍受、再現または不正操作のような活動が確認メカニズムを破壊し得るようなことが高い確率で発生しないようにするため、その確認メカニズムが、電子識別手段の検証のためのセキュリティ管理を実装すること。

2.4. 管理運営及び組織

国境を越える過程において電子識別と関連するサービスを提供する全ての関係者（「プロバイダ」）は、それぞれの構成国における電子識別スキームのための適切な統制組織に対して効果的な実務な存在することの保証を提供するために、文書化された情報セキュリティマネジメントの実務、ポリシー、リスク管理のためのアプローチ、及び、これら以外の承認された管理策をもつものとする。2.4 節全体を通じて、全ての要求事項ないし要素は、所与のレベルにおけるリスクに見合うものとして理解されるものとする。

2.4.1. 総則的な条項

保証レベル	必要な要素
低	1. この規則の適用のある管理運用サービスを提供するプロバイダが、確立された組織をもち、そのサービスの提供と関連する全ての部分において完全に運用可能であることが構成国の国内法によって承認されるような行政機関または法主体であること。 2. プロバイダが、求められ得る情報のタイプ、同一性の証明がいかに行われるか、どの情報をどれだけの期間保持することができるかを含め、そのサービスの管理運営及び提供と関係してそれらのプロバイダに課される法的義務を遵守すること。 3. プロバイダが、損害賠償責任のリスクを予測する能力をもち、並びに、業務運営及びサービス提供の継続性のための十分な資金をもつことを示すことができること。 4. プロバイダが、別の組織にアウトソースした約束の全てを履行することについて責任を負い、かつ、そのプロバイダ自身がその義務を履行するのと同様に、スキームのポリシーを遵守すること。

	5. 国内法によらないで構築された電子識別スキームが、効果的な終了計画をもつこと。そのような計画は、通常のサービス終了または他のプロバイダによる継続、関連する行政機関及びエンドユーザが情報の提供を受ける方法、並びに、そのスキームのポリシーを遵守し、どのように記録が保護され、保持され、破壊されるかに関する詳細を含める。
十分	低のレベルと同じ
高	低のレベルと同じ

2.4.2. 公表される通知及び利用者情報

保証レベル	必要な要素
低	1. 使用上の制限を含め、全ての適用可能な契約条件、要件及び手数料を含める公表されたサービスの定義が存在すること。サービスの定義は、プライバシーポリシーを含める。 2. サービスの定義の変更、及び、特定のサービスに適用される契約条件、要件及びプライバシーポリシーの変更の情報をそのサービスの利用者が適時かつ信頼性のある方法で受けることを確保するために、適切なポリシー及び手順が導入されること。 3. 情報提供の要請に完全かつ正確に対応することを定める適切なポリシー及び手順が導入されること。
十分	低のレベルと同じ
高	低のレベルと同じ

2.4.3. 情報セキュリティマネジメント

保証レベル	必要な要素
低	情報セキュリティ上のリスクのマネジメント及び管理のための効果的な情報セキュリティマネジメントシステムが存在すること。
十分	低のレベルに加え: その情報セキュリティマネジメントシステムが、情報セキュリティ上のリスクのマネジメント及び管理のための実績のある規格または基本原則に附属するものであること。
高	十分のレベルと同じ

2.4.4. 記録の保管

保証レベル	必要な要素
低	1. データ保護及びデータ保持に関する適用可能な立法及びグッドプラクティスを考慮に入れた上で、効果的な記録管理システムを使用して、関連情報を記録し、維持管理すること。

	2. 国内法またはそれ以外の国内行政準則の範囲内で記録し、かつ、監査、セキュリティ侵害の調査及び保持の目的のために必要な期間内、記録を保護し、その後に、その記録が安全に破壊されること。
十分	低のレベルと同じ
高	低のレベルと同じ

2.4.5. 施設及び職員

以下の表は、施設及び職員、並びに、適用可能な場合には、この規則に含まれる義務を負う下請契約者に関する要求事項を示す。その要求事項の遵守は、与えられる保証レベルと関連するリスクのレベルと比例するものとする。

保証レベル	必要な要素
低	1. 彼らが果たすべき役割を実施するために必要な技能において、職員及び下請契約者が十分に訓練を受け、能力を高め、かつ、経験を積むことを確保する手続が存在すること。 2. そのポリシー及び手続に従い、サービスを適切に業務運営するための十分な職員及び下請契約者並びに資金が存在すること。 3. サービスの提供のために使用される施設が、周囲の出来事、無権限アクセス、及び、サービスの安全性に悪影響を与え得るその他の要素を継続的に監視し、それらに対して保護されていること。 4. サービスの提供のために使用される施設が、保有者または処理者の領域、暗号情報その他の機微の情報へのアクセスを、承認を受けた職員または下請契約者に限定されるものとすることを確保すること。
十分	低のレベルと同じ。
高	低のレベルと同じ

2.4.6. 技術上の管理策

保証レベル	必要な要素
低	1. そのサービスの安全性に対して示されるリスクを管理し、処理される情報の機密性、完全性及び可用性を保護するための比例的な技術上の管理策が存在すること。 2. 個人情報及び機微の情報を交換するために使用される電子通信経路が、傍受、不正操作及び再現に対して保護されたものであること。 3. 電子識別手段及び確認の発行のために使用される場合、機微の暗号物件へのアクセスが、アクセスを厳格に必要とする役割及びアプリケーションに制限されていること。そのような物件が平文で長期保存されることが決してないことを確保する。 4. 時間の経過に合わせてセキュリティが維持されること、リスクのレベルの

	変化、インシデント及びセキュリティ侵害に対応する能力があることを確保するための手続が存在すること。 5. 個人情報、暗号情報またはそれ以外の機微の情報を含む全ての媒体が、安全かつ防護された方法で保管され、輸送され、そして、廃棄されること。
十分	低のレベルと同じ。加えて: 電子識別手段及び確認の発行のために使用される場合、機微の暗号物件が、改竄から保護されていること。
高	十分のレベルと同じ

2.4.7. 法令遵守及び監査

保証レベル	必要な要素
低	関連するポリシーの遵守を確保するために、提供されるサービスの供給と関連する全ての部分を含む範囲について、定期的な内部監査が存在すること。
十分	関連するポリシーの遵守を確保するために、提供されるサービスの供給と関連する全ての部分を含む範囲について、定期的な独立の内部監査または外部監査が存在すること。
高	1. 関連するポリシーの遵守を確保するために、提供されるサービスの供給と関連する全ての部分を含む範囲について、定期的な独立の外部監査が存在すること。 2. そのスキームが政府組織によって直接に管理される場合、国内法に従って監査を受けること。