該当箇所の記載方法
(例) 別紙 1 p34 実施要項案 4 章逐条解説 第 6 条 利用者の真偽確認(p3)
上記の例で「p34」は別紙 1 の PDF ファイル全体でのページ番号を示します。
「(p3)」は別紙 1 中の実施要項案のページ下方で表示されるページ番号でパート毎のページ番号を指します。

＜該当箇所＞
別紙 1 p7～p15 有識者会議取りまとめ(案) 5. 制度創設前提論点①(p7)～⑨(p14)

＜意見＞
表題: 制度創設前論点の制度案への反映の不足または不整合

制度の創設にあたり有識者会議において前提論点が整理されていますが、有識者会議が方向性を定めたものについて制度案(規程・実施要項・ガイドライン)に反映されてないか、矛盾しているものが散見されます。

有識者会議での方向性を決めたとしても、最終的な制度案に反映されないのであれば、監督官庁、指定調査機関、認証事業者はそれを遵守する必要がないこととなります。方向性には実効力がなく判断に困り認定調査等に支障が出るのではないでしょうか。認定調査の際の有識者会議取りまとめ(案)の方向性が、結果としてどうなったのか制度案にて規定するか、まとめで方向性を定めたものの規定には反映しなかった旨、明文化を希望します。

・p8 論点① 他制度調査結果援用可否 → 署名法認定認証の調査結果のみ援用を認めるとする記述が規程案、実施要項案、ガイドライン案で言及されていない。
・p9 論点③ トラストアンカー → 総務省でトラステッドリストを発行し情報提供されるとする記述が規程案、実施要項案、ガイドライン案で言及されていない。
・p10 論点④ 他の認証局との併用可否 → 署名法認定認証業務のみ認証局の併用の可能性があることが規程案、実施要項案、ガイドライン案で言及されていない。
・p11 論点⑤ リモート署名・クラウド利用可否 → 電子署名法の範囲を超えないことが規程案、実施要項案、ガイドライン案で言及されていない。リモート署名は認めないとしたがガイドラインではリモート署名に関する言及があるために矛盾が生じており、リモート署名が認められると誤解される恐れがある。

＜該当箇所＞
別紙 p31 有識者会議取りまとめ(案) 7.今後の検討課題(p30)

＜意見＞
表題: 今後の検討課題の早急な解決

今度の検討課題としたもので、今後では間に合わず、告示もしくは調査開始までに規定していないと、認証業務の設計が行えない事項が散見されます。

(1) e シール用認定認証局のトラストモデル、トラストの技術的実現方法
　(1-1) GPKI との相互認証はどうなっているか
　(1-2) 認定認証業務と認定 e シール認証業務の併用の可否
　(1-3) AATL 認証業務との併用の可否
　(1-4) トラステッドリストの発行と運用方法（リストの Acrobat 対応方法を含む）
　これらが規定されていないと認証局の設計ができません。
(2) 共通ポリシーOID の値

これらが実施要項、ガイドラインで規定されることを希望します。

＜該当箇所＞
別紙 1 p9 有識者会議取りまとめ(案) 論点③トラストアンカー(p8)

＜意見＞

表題: PDF で検証容易なトラストアンカー、トラステッドリストの早急な整備

e シールの重要なユースケースは、e シールを付与しデータ発出元が確認できる PDF であり PDF 閲覧ソフトは Acrobat が最も広く利用されていることから、Acrobat で誰でも検証可能であることが必要不可欠であると考えます。

EU の場合には、Acrobat が eIDAS のトラステッドリストに標準対応しており、EU 適格署名・e シールであればデフォルト設定で誰でも検証することができ、また EU 適格であることを視認することができます。

最も望ましいのは総務省や政府が提供するトラステッドリストを Adobe Acrobat で標準対応してもらうよう Adobe 社と交渉し、総務大臣認定 e シール認証業務によって発行された電子証明書に基づいて生成された e シール(以降「認定 e シール」と呼ぶ)であることを区別、視認できることが重要と考えます。また、これができない場合でも、Acrobat が標準で検証できるように AATL 対応などを優先すべきと考えます。

現状の制度案(規程・実施要項・ガイドライン)ではトラステッドリストについて言及されていませんが、有識者会議取りまとめ(案)の方向性の記載されている総務省が提供するトラステッドリストでは、Acrobat では読み込むことができず、多くのユーザーが総務大臣認定 e シールを検証できないという事態になることが危惧されます。認定 e シール用証明書発行事業者の CA 証明書を個別にインスートールすることも可能ですが、これはセキュリティ上推奨すべきではありません。

総務大臣認定タイムスタンプについては、全ての TSA 証明書を発行する全ての認証事業者が AATL 対応しているため、認定タイムスタンプの PDF の検証で問題が起きることはありませんでした。

署名法の認定認証事業者の場合には、GPKI ブリッジ CA と相互認証されているのでトラストアンカーの問題が発生しません。

(制度創設前論点の方向性より)認定 e シールの場合には、GPKI ブリッジ CA と相互接続せず、総務省の提供するトラステッドリストを使用するとしたために、特別な手当てが必要であることに留意ください。

現状の制度ままでは、認定 e シールの PDF は Acrobat で閲覧した場合、全て検証結果無効と判断され、利用者、事業者にとってメリットの無い制度となってしまいます。

＜該当箇所＞
別紙 1 p15 有識者会議取りまとめ(案) 論点⑨セキュリティレベル(p14)

＜意見＞
表題: より広く利用しやすい認定 e シールのセキュリティレベル設定

認定 e シールの多くの利用が想定されるユースケースとしては
・企業がその企業から送信された PDF であること証明するためにサーバーで大量の PDF に認定 e シールを付与する。
・複数人の企業の担当者が認定 e シールをつけた PDF を作成、送信する。
など、署名法認定認証による電子署名と異なり、もう少し気軽に e シールを付与するケースの方が多いのではないかと考えており、利用者が適切に管理されていれば、サーバー側で HSM や USB トークン等を使わずに e シールを付与したり、複数人で利用できるようにしたりしても良いように思います。

このようなライトな利用の必要性は一昨年の総務省 e シール有識者会議でも委員の方がコメントされていたと記憶しています。

その一方で、有識者会議の方針としては認定 e シールを署名法認定認証のセキュリティレベルを求めるとしており、主要な想定利用ケースに対して過度な要件であると考えます。

e シール用認定認証業務の制度設計は、署名法の認定認証に加え、総務大臣認定タイムスタンプで定められた要件も加えられており、署名法の認定認証業務の制度よりも事実上、より高いセキュリティレベルを求めることになってしまっており、市場の要求、期待と大きく乖離しているように思います。セキュリティレベル設定の再考を希望します。 また、認定認証業務に対して過度なセキュリティ要求を設けているのに対して、e シールを付与する利用者に対してセキュリティ要求はなく、セキュリティレベルの設定が整合していないように見受けられます。
＜該当箇所＞ 別紙 1 p11 有識者会議取りまとめ(案) 論点⑤方向性 リモート e シール(p10) 別紙 1 p67 ガイドライン 3 章 用語集(p10) 別紙 1 p72 ガイドライン 4 章逐条解説 第 7 条 (2)条文解説 ①利用者等(p15) ＜意見＞ 表題: リモート認定 e シールの利用可否の明確化 有識者会議で示された方向性では、リモート e シールについて電子署名法の範囲を超えて制度で記載しないとの方針が示されましたが、ガイドラインの用語集ではリモート e シールについて記載されており、制度上認められているかのような誤解を受けます。 リモート e シールについては、利用者の秘密鍵を受託管理する信頼に足りるリモート e シール側の要件や制度が整っていない中、リモート e シールを制度として認めることは尚早であると考えており、ガイドラインにおいて、現時点の制度ではリモート e シールは認めないことを改訂が比較的容易なガイドラインの中で規定すべきと考えます。
＜該当箇所＞ 別紙 1 p8 有識者会議取りまとめ(案) 論点①他の認定調査の援用(p7) 別紙 1 p10 有識者会議取りまとめ(案) 論点④認証局の併用(p9) ＜意見＞ 表題: PDF 検証容易性の促進のための他の認定調査の援用 PDF による認定 e シールを考えた場合、Acrobat では総務省トラステッドリストは標準搭載されないか、搭載されるとしてもその調整には数年の Adobe 社との調整が必要になると考えております。 そのような空白期間を埋めるためにも Acrobat 標準搭載の AATL トラステッドリストに含まれる認証局が総務大臣認定取得することを促進するような施策、制度が必要であると考えており、以下が必要と考えます。 (1) AATL 認証局との併用 (2) AATL 認定取得済認証局の調査の緩和、省略 現状の有識者会議では以下のように方向付けられました。 ・認証局の併用は署名法認定認証局としか可能性がなく AATL 認定認証局との併用はできない(まとめ論点④) ・AATL 認定の調査結果を用いて e シール用認証業務の認定調査へ援用などの軽減措置は取らない(まとめ論点①) しかしながら、これらの方向性は実施要項案、ガイドライン案には反映されておりません。 有識者会議の方向性では、AATL は「民間の認定制度であるため、関係規程にその技術要件を反映することはしない」としていますが、AATL の技術要件は、米国公認会計士協会及びカナダ勅許会計士協会によって 共同開発された電子商取引認証局監査 プログラム(WebTrust for CA)や欧州電気通信標準化機構(ETSI)の規格 に基づく認証局の監査などを援用しています。それらは電子署名法の認定要件の大部分で整合しているため、WebTrust for CA や ETSI の認証局監査結果を援用可とすることを希望します。

このような AATL 促進施策が行われないと認定 e シールが付与された PDF を Acrobat で閲覧した場合、全て検証結果無効と判断され、利用者、事業者にとってメリットの無い制度となってしまいます。

尚、直ちに援用可と判断できない場合は、認定 e シールの制度と、WebTrust for CA や ETSI の規格との差異を明らかにするような調査、検討を行い AATL 援用い向けた促進策を行うべきであると考えます。他の認定制度を例にとると、電子委任状法の基本指針では電子署名法の認定とならび、こちらの 2 つの監査のどちらかを年 1 回以上受けることも認定要件に組み込まれています。

＜該当箇所＞
別紙 1 p10 有識者会議取りまとめ(案) 論点④署名法認定認証との認証局の併用(p9)

＜意見＞
表題: 署名法認定認証業務の認証局併用に関する制度案への反映

認定認証業務は電子署名法において認証局の併用を認めていないので、総務大臣認定 e シール認証局の併用もまた認められないのではないでしょうか。認定認証業務認証局ならば e シールとの併用は可能であるかのような方向性の記述は誤解を受けるのではないでしょうか。デジタル庁との調整の結果、規程案、実施要項案、ガイドラインには反映されていないようですが、認証局の併用について規定する必要があると考えます。

＜該当箇所＞
別紙 1 p36 実施要項案 4 章逐条解説 第 7 条第 1 項第五号ト 共通ポリシーOID(p5)

＜意見＞
表題: ガイドラインでの検証可能な共通ポリシーOID に関する規定

総務大臣認定を受けた認証事業者の発行する e シール用電子証明書であることを示すために、利用者証明書(エンドエンティティ証明書)の証明書ポリシーに共通ポリシーOID が記載されることが実施要項で示されましたが、証明書ポリシーは連鎖の検証の結果有効なものである必要があり、当該箇所には「有効な」等、補足して記載する必要があり、ガイドライン等でその技術的な補足解説が必要と考えます。
具体的には、認証局がルート CA、下位 CA(中間 CA)、利用者証明書の階層モデルであった際に、中間 CA の証明書ポリシー群には共通ポリシーOID が記載されるか、任意のポリシー(anyPolicy)を許可するように設定されていなければなりません。
「有効な」ポリシーが設定されなかった場合、e シール用電子証明書の検証が失敗し無効と判断されます。

＜該当箇所＞
別紙 1 p14 有識者会議取りまとめ(案) 論点⑧ eKYC 可否(p13)
別紙 1 p34 実施要項案 4 章逐条解説 第 6 条 利用者の真偽確認(p3)

＜意見＞
表題: マイナンバーeKYC の導入による利用者審査負担の軽減

総務大臣認定 e シールではオンライン本人確認(eKYC)の利用を認めないとされていますが、署名法認定認証でマイナンバーカードを用いてオンラインで本人確認(eKYC)を行っている事例が既にあるのではないでしょうか。また、組織の実在確認では国税庁の法人番号公表サイトが利用できます。

利用者申請がオンラインで完結することも可能な、利用者および認定事業者の負担軽減や利便性向上した制度設計を希望します。

＜該当箇所＞
別紙 p33 実施要項案 4 章逐条解説 第 4 条 暗号技術(p2)

＜意見＞
表題: CRYPTREC 暗号リスト準拠に関する適切な適用範囲の設定

第 4 条では「e シールの付与対象となる電子データのハッシュ値を得るためのハッシュ関数および公開鍵暗号(署名)」について規定していますが、タイムスタンプと異なり、このハッシュ関数と署名アルゴリズムは e シールを作成する利用者のシステムが決めるものであって、認証事業者が強制できるものではないため規定から削除すべきと考えます。

一方で、規程 第 3 条「利用者だけが付与又は関連付けることができる」とあるので、実施要項 第 4 条では、e シール用電子証明書だけでなく、ルート証明書からのチェーン、失効情報を含め暗号が CRYPTREC 暗号リスト準拠である必要があると考えます。

＜該当箇所＞
別紙 1 p9 有識者会議取りまとめ(案) 論点③トラストアンカー(p8)

＜意見＞
表題: 日本政府としてのトラストアンカー、トラステッドリスト掲載の促進

総務省が発行するトラステッドリストは将来的には、総務省だけでなく日本政府として発行されるものとし、国際相互承認が可能となることを目指すべきであると考えます。

＜該当箇所＞
別紙 1 p36 実施要項案 4 章逐条解説 第 7 条 第 5 号 証明書記載事項 チ(p5)

＜意見＞
表題: 利用者 e シール符号の利用目的の制限の補足、明確化

実施要項案では求められる証明書記載事項に「チ 利用者 e シール符号の利用目的の制限を示す情報」とあり、証明書の keyUsage 拡張のことを指していると思われますが、指定調査による調査の際に容易に判断ができるようにその設定可能な具体的な値について、実施要項もしくはガイドラインで規定しておく必要があると考えます。

ちなみに、欧州の法人用証明書プロファイルの規格 ETSI EN 319 412-3 v1.3.1 では、
一般の e シール用電子証明書では nonRepudiation、digitalSignature、
keyEncipherment/keyAgreement ビットを使うことができ、欧州適格 e シールでは
nonRepudiation ビットのみを使うもの(shall)としています。

但し、Java では nonRepudiation ビットのみの証明書で署名検証するとエラーになるため、日本の認定 e シールでは nonRepudiation と digitalSignature ビットのみを有効にした keyUsage 拡張を設定すべきと考えます。

＜該当箇所＞
なし

＜意見＞
表題: 利用者の鍵管理義務の記載不足

e シール生成者である利用者の鍵管理義務について、告示、実施要項およびガイドラインで一切言及されておらず、利用者の鍵管理義務について規定する必要があると考えます。

この規定が無いために、USB トークンやスマートカードを必須とするのか、PKCS#12 ファイル渡しでもよいのか、リモート e シールでも許されるのかなど判断がつきません。

参考まで、電子署名法の認定認証業務においては、これでは不十分とも思いますが「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針 第 8 条」において、認証事業者が利用申込み者に管理義務を負うことの説明義務を設けています。

いくら認定認証業務のセキュリティ保証レベルを上げたとしても、杜撰な利用者鍵管理が許されてしまうと制度の信頼自体が揺らいでしまいます。