電子署名法認定基準のモダナイズ検討会（第１回）議事要旨

1. 日時
   令和 6 年 9 月 20 日(金) 13:00～15:00

2. 場所
   オンライン開催

3. 出席者
   開催要領のとおりにつき省略

4. 議事
   (1) 電子署名法について
   (2) 昨年度事業の振り返り
   (3) 本検討会における検討の方針と内容
   (4) モダナイズの方向性①と②に関する議論
   (5) 次回以降の進め方について

5. 議事概要

はじめに

- 委員の互選により松本座長を選任

(1) 電子署名法について

【松本座長】

- 電子署名法は 2000 年に成立し、2001 年に施行された。当時は電子社会のビジョンが語られ、その実現を支える法制度として設けられたが、現在では技術やセキュリティの考え方が大きく変化している
- 特に、欧州連合（EU）における 1999 年の電子署名指令は、日本の電子署名法に大きな影響を与えているが、この欧州電子署名指令は既に大きく変貌している。2014 年には、eIDAS 規則と指令から規則となり、今年 2024 年には eIDAS2.0 として更に大きく改正されており、日本としても国際基準に準じた法整備を進める必要がある
- 電子署名法が制定された当時の技術やセキュリティ要件と、現在のデジタル社会における要件は大きく異なるため、認定基準を最新化し、国際的な基準との整合性を図ることが急務である

(2) 昨年度事業の振り返り

- 昨年度の検討会では、特定認証業務の認定基準の見直しに向けて、現行基準の課題が明確化された。これに基づき、6 つの主要な論点が設定され、議論が行われた

(3) 本検討会における検討の方針と内容

【宮内委員】

- 今回の会議の目的は、可能な部分から検討を進め、長期にわたる課題は別に扱うという趣旨であった。しかし、この議論ではそれ以外にも考慮すべき点が多く含まれている。必ずしも個別の論点だけにこだわらず、もう少し長期的な視点で検討を行うべきである。以下の 3 点をコメントとする
  1. 現在の法令構造について、JIPDEC の指定調査期間への通知に重要な事項を記載するのは今後も適切かどうか再検討する必要がある。技術的な要件は、デジタル庁内でなく、専門の部局や機関が担当する形も検討すべき
  2. AATL などの国際基準に適合し、一般的なツールで検証できることが重要であり、これらとの関係性を考慮して進めるべき
  3. 現行の施行規則では、リモート署名で生成された鍵ペアの公開鍵を認定認証業務が受け取れない問題があるが、リモート署名に関する議論をこの会議で進めるのか確認したい

【宮内委員】

- 事務局の回答の 1 点目について、追加でコメントする
  1. 現在の通知の構造でも問題はないとの理解だが、指定調査機関が複数となる可能性を考慮すると、特定の機関への通知は望ましくないため、中長期的にはこの点を見直すべき

【小田嶋委員】

- 事務局へ以下の 3 点、質問と意見をコメントする
  1. リモート署名については長期的な課題として来年度以降に継続検討されるのか、今後の方針を教えてほしい
  2. 昨年度の調査研究で 6 つの課題以外にも提案事項があったが、それらも来年以降に継続実施されるのか確認したい
  3. 認定認証事業者の意見では、④の優先度が最も高いとのことで、今年度中に検討され来年度施行が望ましい

【満塩委員】

- 電子署名法全体の構造についても、今後の技術進展を考慮しながら、リモート署名やクラウド技術、さらには AI の導入を見据えた意見交換の場を設けるべき。特に、日米デジタル貿易協定に関連する電子署名の議論について、適切なタイミングで意見を述べたい

- 認定基準のモダナイズに加え、認定制度のスキームそのものを再検討する必要があると考える

(4) モダナイズの方向性①と②に関する議論

課題① 国際基準に照らし合わせた情報セキュリティに関するリスクマネジメントの規定

【漆嶌委員】

1. 現行の法律・指針・施行規則にリスクマネジメントが含まれていないのに、後から含まれていたと主張するのは難しい。法律は変えず、指針や施行規則に情報セキュリティマネジメントを明記し、義務付けるべきである
2. ETSI に基づくリスクマネジメントを導入するという議論に違和感がある。ISMS の観点から、リスクマネジメントは国際規格に照らして行うべきであり、ETSI に習う必要はない
3. 事業者によってリスク評価や遂行能力にばらつきがある点が懸念される。リスク評価方法や対策は ISMS やガイドラインに基づき統一された基準で行うべきである
4. 認定認証事業における共通のリスクファクターを基に、事業者に同じ基準で確認を行わせるのが望ましい。既に対策済みのものは不要だが、抜け漏れのリスクはしっかり確認する必要がある

【松本座長】

- 漆嶌委員の 1 点目について以下のようにコメントする
  1. 電子署名法は 2000 年に制定され、ISMS や IT-BCP の国際標準はその後に登場したため、後付けの対策では十分ではない可能性がある。さらに、ETSI は認証局のインシデントに対応して基準を改定してきたが、そうした枠組みがなかったことが問題であったと考えられる

【JIPDEC 大澤様】

- サイバー攻撃が頻発している現状では、電子署名法が制定された当初よりも、重要インフラに対する対策が一般的になっていると考える
- 認定認証業務用設備は現在重要インフラには含まれていないが、セキュリティ上の観点からリスクマネジメントが必要であるという問題意識がある

【松本座長】

- 欧州の NIS 2 指令では、デジタルインフラストラクチャにトラストサービスが含まれており、重要インフラとして認証局に新たな要件が課せられることが国際的な流れになっていると感じた

- ISMS は一般的な情報システムに適用されるが、認証局はそのアーキテクチャが明確で、守られる仕組みが既に内在している。2000 年に作られた電子署名法の基準も網羅的だが、一部足りない部分があると考えられる

【満塩委員】

- リスクマネジメント導入ではなく、ガバナンス基準導入の話ではないか？私のイメージでは、リスクマネジメントはガバナンス基準の一部に含まれるものであり、リスクマネジメントという言葉だけだと、PDCA サイクルが本当に適用されるのか疑問が残るため、ガバナンス基準の方が適切ではないかと考える
- ガバナンスというイメージで以下 2 点コメントする
  1. 電子署名法は 2001 年に施行されたが、ガバナンスという概念は当時あまり取り入れられていなかったため、現在の重要性を踏まえ、ガバナンスを導入するべきだと考える。法改正なしにガバナンスが入る解釈も可能だが、法施行的には外出しするのが望ましい
  2. 基準に関しては、ETSI の基準だけを参考にするのではなく、ISMS や ISMAP のガバナンス基準、マネジメント基準、管理策基準を参考にすべきである。また、経産省のシステム監査基準におけるガバナンス項目も考慮するのが適切であると考える

【小田嶋委員】

- 以下 3 点コメントする
  1. 法規則第 6 条第 1 項第 15 号は主に認証局の秘密鍵の危殆化に関する事項に限られており、リスクマネジメントやガバナンスに関する事項は厳密には含まれていないと考えている
  2. 法の改正は難しいが、現実に含まれていない部分を反映することが望ましく、デジタル庁の負担を軽減しつつ修正する方法を検討すべきである
  3. 認証局や指定調査機関が実施・調査する際にはコスト低減が重要であり、リスクマネジメントのガバナンス要素を取り入れ、最終的には会社のトップレベルでリスクを承認する体制が必要だと考える

【宮内委員】

- 法律を変える必要はないが、施行規則は変えたほうが良いと考える
  - 法第 6 条第 1 項第 3 号は非常に広い範囲をカバーしているため、リスクマネジメントを追加しても含まれると考え、法律自体の改正は不要だが、施行規則の第 15 号トは狭く理解されているため、これを改正すべきである
  - リスクマネジメントやガバナンスを施行規則に明示するために、文言を改正するか、新たに項目を追加することで、施行規則を変更すべきであると考える

【漆嶌委員】

- 満塩委員のガバナンス導入の提案について、国際相互承認の観点では WebTrust や ETSI などの規格でリスクマネジメントが明文化されていることが重要であり、電子署名法の認定基準でもリスクマネジメントが実施されていることを明示するべきであると考える
- ガバナンスについては、CP/CPS 全体に既に関連事項が散りばめられており、ガバナンスを一言で明記するのは難しいと考えている

課題② 認証局の秘密鍵を管理する暗号装置の技術基準の更新

【漆嶌委員】

- 現在は FIPS 140-2 から 140-3 への移行期であり、140-3 の製品がまだ十分出揃っていないため、現時点では 140-2 と 140-3 の製品を併用するのが適切と考える
- FIPS の期限切れリスクを考慮し、申請時や調査時、運用過程で FIPS が期限切れになる場合の対応を明確化する必要がある
- 認証局の HSM が瑕疵により Revoked（取り消し）されるケースと、関係ない理由で Revoked や Historical（過去の状態）になるケースを区別し、運用に影響がない場合は使用を継続できる基準を明確化するべき
- FIPS 140 の Level-3 以上、Common Criteria の EAL4+以上などのレベル設定について、基準での明確化が必要であると考える

【満塩委員】

- 質問として、審査時に FIPS の認証書を確認しているかどうかを確認したい。FIPS が明記されていなくても、内容を日本語で書き下したものが使われていると理解しており、これは 2001 年頃のやむを得ない対応だったと聞いている。現在では、〇〇Level 以上や認証書を明示的に記述しても良いと考える
- FIPS が日本の制度ではない点も理解しているが、ISO などで表記できるならば、そちらを使用することも検討すべきだと思う。以上の点で記述の改善を求めたい

【松本座長】

- 2000 年当時、日本には国産の HSM が各社存在していたが、その後撤退してしまった。今年の CRYPTREC で日本製 HSM がないことが嘆かれたが、日本に HSM が存在しないことは産業政策上好ましくない
- HSM に多くのトラストアンカーが繋がっている状況で、国産 HSM がないのは好ましくないが、認証局の立場からすれば、FIPS140 を取得した HSM を採用することがデファクトスタンダードになっているため、大きな問題はない
- しかし、HSM の重要性は再認識すべきであり、国産 HSM の不在がもたらす影響についても再考する必要がある

【JIPDEC 大澤様】

- 確かに FIPS140-1 や 140-2 の認証を確認しているが、現在の指針には暗号装置の技術基準についての言及がない。指定調査機関はデジタル庁や法務省民事局から示された方針に基づいて、暗号装置の信頼性を確認している
- この方針は、具体的な技術基準というよりも、2001 年当時の FIPS140-1 のセキュリティ要件に基づいて書かれたものである
- 世界の認証局はすでに FIPS140-2 や 140-3 へ移行しているため、JIPDEC としても数年前から主務省庁に対し、認定基準を早急に明確化し、指針に反映するよう要望している

【小田嶋委員】

- FIPS140-2 から 140-3 への移行過渡期にあたり、認証局としても対応に困っている。140-2 を選ぶと将来的に問題が生じる一方、140-3 は簡単に入手できない状況にある
- CA システムを提供するベンダーの対応も困難な場合があり、暗号移行も控えているため、HSM の対応は簡単ではない。主務省に最終判断を仰ぐ必要があると考えている
- 認定認証事業者の事業継続性は重要であり、コストが撤退の要因となることもある。モダナイズの必要性を認識しつつも、事業継続性やコスト負担を考慮して進めるべきだと思う

(5) 次回以降の進め方について

【松本座長】

- 次回の議論では、クラウドサービスの利用や遠隔操作の許容が大きな焦点となり、これらの技術的課題に対応する基準整備が進むことで、日本の認証局の競争力向上につながると期待される。技術基準のモダナイズを通じて、国際基準との整合性を確保しつつ、日本のデジタル社会の発展を支える基盤整備を目指す

【小田嶋委員】

- スケジュールについて、第 4 回が 12 月頃で、早ければ来年 4 月に施行されると聞いたが、具体的な日程を確認したい。パブリックコメントや指定調査機関の調査時期、調査票の修正期間など、影響が想定される時期についても教えてほしい。特に、今回の内容が調査手数料や調査機関の金額に影響するか確認したい
- ガバナンスについて、施行規則の第 6 条 15 号ロに「業務従事する者の責任および権限、指揮命令系統」の記述があるが、これがガバナンスの観点からふさわしい内容か検討するべきかもしれないと感じた

以上