追加アンケート結果及び事務局案

資料2

※凡例

実現可能と思われる事項: ○
実現可能と思われるものの、個別具体的な検討が必要と思われる事項: △
実現可能性について本研究会で検討が必要と思われる事項: P

項番	追加のご意見・ご質問	JIPDEC案	事務局案
3821 3822	「平成23年度 電子署名法研究会」において、暗号アルゴリズム移行のフェーズ2の期間に各事業者がコンテンジェンシープラン発動時に実施する「緊急時対応計画」に関する議論がありました。緊急時対応計画実施時には、全ての利用者証明書の失効が必要になりますが、殆どの事業者が、「電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該電子証明書の利用者にその旨を通知すること（施行規則第六条第十二号）」に基づき、特定記録郵便、簡易書留等により本人に確実に届く手段で個別に失効通知を郵送している実態が確認できました。 研究会の時には、それぞれの事業者で全失効に要する作業期間の見積のアンケートなども実施され、失効処理は認証局システムの機能でCSVファイル投入などの一括処理が可能であるが、利用者への失効通知の郵送が手作業になるため、数ケ月から事業者によっては年単位になる事業者もあり現実的ではないとの議論がありました。しかし、その時点では（施行規則第六条第十二号）があるため、何らかの個別の失効通知は必要との見解のまま特別な結論を導き出すには至っておりません。 この研究会では最終的に「緊急時対応計画雛型」が示され、認定の対象としないながらも、「緊急時対応計画」の作成の指示があり、その後、作成状況の確認も実施されており、各事業者が独自に「緊急時対応計画」を策定しており、失効通知の方法は事業者側に託された形のままとなっています。 その後、近年になって閉局時に一括して利用者証明書を全失効するケースがあり、事実上、コンテンジェンシープラン発動に近い処理を実施している認証事業者が存在しています。この一括失効の実施に当たっては、証明書利用者に個別の失効通知を郵送するのではなく、全証明書利用者が所属する団体の会員に対する会報への掲載で失効通知に代えるなどの代替案も出て来ています。 このような昨今の状況を踏まえて、暗号アルゴリズム移行も一段落したところで、今一度、コンテンジェンシープラン発動時の「緊急時対応計画」実施時の失効通知のやり方に関して、議論させていただきたいと思います。	左記にもあるように、施行規則第六条第十二号において利用者への失効通知義務が求められているため、何らかの失効通知が必要であることに代わりはないと思われる。 SHA-2移行が順調に推移した今日、「緊急時対応計画」実施時の失効通知のやり方に関する議論よりも優先する課題があると思料する。	主務省としては、全利用者に失効通知がされていれば法令上問題はなく、具体的な通知方法については平時であっても，コンティンジェンシープラン発動時であっても、認定の対象外と考える。

項番	追加のご意見・ご質問	JIPDEC案	事務局案
3511、 3513、 3711、 3712、 3713、 3811、 3812、 3901、 3907、 3909、 390B、 390D、 3A02、 3A03、 3C56、 3C62、 3C63、 3E21、 3E22、 3E23、 3E24、 3E41、 3E42、 3E43	近年、外部事業者のサービス、或いは関連会社のサービスとして、クラウドサービスを中心に従来とは異なる各種のサービスが提供され、利用可能な場面が多くなってきています。特に2011年以降には、災害対策のBCPの重要性が大きく見直され、BCP対策として単純なバックアップサイトというよりクラウドサービスを利用した遠隔地への二拠点／複数拠点化、或いは回線を利用した遠隔地バックアップを実現するサービスなども登場しています。認定認証事業者から見て、認証局秘密鍵を格納する「認証設備室」を外部サービスの利用やクラウド化するような考え方には無理がありますが、認証業務用設備以外の汎用的なシステムをクラウド化することは利用価値が高いものも考えられます。例えば以下のような例が考えられます。 1） 業務データ（運用規程、手順書、設計書等）を保管するファイルサーバとしてストレージサービスを利用 2） 利用者からWebシステムで利用申込データ等を入力する時のWebサーバ 3） リポジトリサーバのスタンバイ機を遠隔地に設置しDNS切替で運用 4） 遠隔地バックアップサービス（回線利用／オフライン）の利用による認証局サーバ復旧のためのデータのバックアップ保管 現在のJIPDECの認定調査では調査表項番には明示されていませんが、運用規程を保管するファイルサーバの設置場所と、そのファイルサーバへのアクセス権限を確認することが実施されていたり、また外部サービスを利用する場合、業務委託先ということにもなるため委託契約書の他、委託業務の実施場所の確認が必要になっています。しかるにセキュリティ上の理由からクラウド事業者が設置場所を明らかにしない場合、またサービスの実装によってはサービス提供側にも特定が困難な場合もあり得るようになっています。認定認証業務における委託先の完全な設置場所の調査の実施という方法があるがために認定認証事業者がBCP対策として、このようなストレージサービスやクラウドサービスの利用を見送っているケースもあり、これがそのまま有効なBCP対策の実施、認証業務の維持の阻害要因になっています。近年の現状を鑑み、BCP対策として有効と思われる外部サービスの利用可否に関して、設置場所の調査の必要性、外部サービス等の申込書、委託契約書、SLAレベルの内容確認に代えることの可否について議論させて頂きたくお願い致します。	規則第四条に定められた認証設備室等の厳しい要件があるが、左記ご意見1)から3)のように、認証設備室や認証業務用設備に関わらない設備の要件であれば、クラウドサービスを活用する余地があると思われ、研究会の場でご議論いただくことがよいと思料する。 ただし、4) については、本来認証設備室の中でのみ守られるべきデータであるため、1)から3)よりも慎重な検討が必要であると考えられるところ、調査表3C56の要件にて、保存場所の安全性を確認する必要があると思料する。	ご意見では「認証業務用設備以外の汎用的なシステム」とされているが、4)は遠隔地バックアップでサービスの利用による認証局サーバ復旧のためのデータのバックアップ保管に係るものであり、指針14条2号が適用されると考える。 バックアップデータの保存方法を規定した法令は存在しないが、バックアップデータの重要性は特に高いものであり、3C56の要件により保存することに問題はないと考える。 なお、4)については、電子署名法施行規則6条17号の趣旨に鑑み、認定認証事業者においてデータセンタの所在場所の確認は必要と考える。経済産業省所管のクラウドセキュリティガイドライン10.1や付属書Aなどでも、データセンタの所在についてクラウド事業者は情報開示すべきであるし、クラウド利用者は確認すべきとされているところ。

項番	追加のご意見・ご質問	JIPDEC案	事務局案
3C21、 3C22、 3C23、 3C62、 3C63、 3E21、 3E22、 3E23、 3E24、 3E41、 3E42、 3E43	秘密鍵の秘密分散データ(鍵断片)のバックアップ保管において、遠隔地バックアップ保管サービスを利用することについて議論して頂きたいと思います。	指針第十四条第二号イによらず、同条同号ロの方法によって秘密分散されたバックアップデータであれば、その一部のみについて遠隔地バックアップ保管サービスを利用することは可能であると思料する。 その場合、1枚については必ず、RA又はIAの金庫等に保存することとし、また遠隔地バックアップ保管サービス利用時に2枚以上のバックアップを遠隔地保管してはいけないこととし、遠隔地バックアップ保管サービスに保存されたバックアップのみで復元することができないように担保させることが望ましいものと思料する。 ただその場合、RA又はIAが被災すると、遠隔地のバックアップのみでは復元できなくなるリスクが生じる。 発行者署名符号の重要性を考慮した場合、遠隔地バックアップ保管サービスは利用すべきではないと思料する。 また、遠隔地バックアップ保管サービスを利用してバックアップを保管することを認める場合においても、利用する「秘密分散方式」の安全性を複数の有識者(専門家)による評価を実施し、その安全性に問題がないことが確認された方式を用いることが望ましいと思料する。	指針14条第2号ロによって、発行者署名符号に関する情報を分割し、複数の者が異なる安全な場所に分散し保管することは可能であるので、遠隔地バックアップ保管サービスを利用することは可能と考える。 一方で、遠隔地バックアップ保管サービスを利用することによるリスクが発生することはJIPDEC案のとおりであり、同サービスを利用する場合には、リスクを十分に分析し、受容できる範囲内か検証する必要がある。

項番	追加のご意見・ご質問	JIPDEC案	事務局案
3C21、 3C22、 3C23、 3C62、 3C63、 3E21、 3E22、 3E23、 3E24、 3E41、 3E42、 3E43	認証設備室のDRサイトを構築することは非常に大きな設備投資が必要になり、実現が大変困難です。但し、災害発生時に認証設備室内のサーバは大破したが、認証設備室はセキュリティ装置等の修理で使用可能なような場合も考えられます。 このようなケースに対応する一つの考え方に、認証局秘密鍵のバックアップ保管の一つの手段として、秘密鍵が格納されたHSMを含む代替機サーバを遠隔地にコールドスタンバイ機として保存しておきます。コールドスタンバイ機ながら、有効な認証局秘密鍵が複数存在することになりますが、この代替機を災害発生時に、遠隔地からセキュリティ上の措置を持って搬送することにより、システム復旧を図るという考え方が考えられます。この考え方の是非について議論して頂きたいと思います。	規則第四条第一号により、認証業務用設備は認証設備室に設置されている必要があるので、発行者署名符号が格納されたHSMを含む代替機サーバを遠隔地にコールドスタンバイ機として保存したい場合には、当該遠隔地について認証設備室として認定を取得することで可能になると思料する。	HSMを含む代替機サーバを遠隔地にコールドスタンバイ機として保存したい場合には、認証業務用設備と考えられる以上、正式に認定を受けた上で設備として利用していただく必要があると考える。
4101 4102 4103 4104 4105 4106	施行規則第12条第1項第1号、同第2号、同第三号について 以上当該帳簿書類は施行規則第12条第2項により「当該帳簿書類に係る電子証明書の有効期間の満了日から十年間保存しなければならない。」が、申込総数によっては保存場所の確保などに難儀する。 法人の取引記録・帳簿書類は事業年度の確定申告書の提出期限から7年間保存であり、10年は過度のものと想定される。	本件については、すでに第2回の研究会の中で主務省より現行保存期間を維持すべきとの見解が示され、大きな反対意見は出なかったと理解している。	10年という期間は、民法の時効の規定に従ったもの（167条1項）。現在進められている民法改正の議論を注視したい。

項番	追加のご意見・ご質問	JIPDEC案	事務局案
2000番台	組織内個人の証明書の法的位置づけについて，以下の点を検討すべきである。 【電子取引において電子証明書により証明すべき内容】 BtoB及びBtoCでの利用を考えると，組織（企業，法人）内の個人の電子証明書が重要である。 取引にあたって重要なのは，ある個人による意思表示による効果が所属組織に帰属するか否かである。したがって，組織への所属や，組織内での部門・役職等の確認が，取引においては重要であり，当該個人の住民票上の記載情報は大きな意味をもたないといえる。 なお，適切な役職名のついた電子証明書にもとづく署名があり，組織を代理するものと署名の受領者が信用するに値する状況であれば，会社法14条1項又は商法25条1項の使用人の包括代理権（場合によっては民法109条等の表見代理)により，意思表示の効果は組織に帰属するものと考えられる。 【本人確認の内容】 電子取引における本人確認においては，住民票の確認ではなく，取引に関する権限の指標となる情報としての所属・役職等の確認が必要となる（本人たるアイデンティティが，住民票記載の自然人なのか，社会的活動におけるアイデンティティなのか，という問題ともいえる)。最終的に，電子証明書に基づく意思表示の効果が組織に帰属することの根拠となることを目的とするのであれば，本人確認や電子証明書・秘密情報の管理の責任は当該組織に負わせればよい。したがって，認証事業者としては，組織代表者等，組織の意思表示のできる者からの情報にもとづいて電子証明書を発行すればよく，住民票上の個人と同一であることを確認する必要は乏しいか全くないものと思われる。（仮に，かかる情報に誤りがあったとしても，それは，当該組織の責任となる）。 【まとめ】 組織が組織の責任で組織内個人の証明書（所属，役職等を記載したもの）の発行を申請し，これにもとづいて認証事業者は電子証明書を発行する。申請内容に誤りがあったとしても，それは申請元組織の責任であって，認証事業者の責任ではない。このような電子証明書の発行を行うべく，法令改正を検討すべきである。	調査表3602の適合例に記述され、電子署名法に基づく指定調査機関の調査に関する方針第4の4.にも規定された「電子証明書に利用者の役職名その他の利用者の属性が署名法の認定対象外である」ことの是非については、第1回の研究会でも検討が重ねられ、さらに弁護士を含む多くの構成員からこのような意見が上がってくることを重視し、署名法にとってのあるべき姿を示す時期に来ているものと思料する。 指定調査機関としての考え方は、「認定認証業務により発行された電子証明書の本来の利用方法に合わせ、属性情報の真偽確認方法についても認定の対象として明確かつ適切に規定し、法の体系を利用実態に合わせることが望ましい」とする考えに変更はない。	現行法の枠内では対応は困難である。 来年度以降、引き続き継続して検討したい。
3600番台	「電子証明書に記載される利用者の属性」に対する認定について 施行規則第6条第8号 現状、利用者（自然人）の「氏名・生年月日・住所」以外の属性は認定の対象外であるが、電子証明書が主にビジネスで利用される場合は、法人名、所在地などのデータが重要であり、現状において商業登記簿の提出を求め、かつその記載どおりに電子証明書へ格納している。 認定認証事業者の発行する電子証明書は、「企業内個人」としての利用され、利用者が組織への所属が関係ない電子申請（例えば、体育館の利用申請など）の場合は「公的個人認証サービス」という棲み分けとなっているが、属性の認定範囲は同一であり、その意味で区別はつきにくい。属性に関して認定対象とし、公的個人認証Sサービスと明確な区別を行いたい。 ※個人の属性としては、法人を含む組織として法人名（組織名）や所在地、あるいは平成28年1月より利用される法人番号（国税庁が付番するもの）なども考えられる。	調査表3602の適合例に記述され、電子署名法に基づく指定調査機関の調査に関する方針第4の4.にも規定された「電子証明書に利用者の役職名その他の利用者の属性が署名法の認定対象外である」ことの是非については、第1回の研究	

項番	追加のご意見・ご質問	JIPDEC案	事務局案
360O番台	「2) 電子証明書に利用者の役職名その他の利用者の属性（利用者の氏名、住所及び生年月日を除く。）は電子署名法(電子署名及び認証業務に関する法律)における認定の対象外であることを電子証明書に注記している、又はその情報へのリンク先を電子証明書に記録している。」とあるが、実状では属性を記載した証明書や、住所等の情報を記載しない証明書など様々な形態の証明書が有用であるケースも多いため、利用場面に応じた証明書が選択可能であるべきである。 論点としては、以下のものが考えられる。 ・<u>属性を記載した証明書の属性部分も範囲に含める検討。</u> 証明書プロファイルに署名者の属性を記載する場合の認定基準の検討。 例：法人名・組織名、資格属性（各士業、建築士など）、法人番号、など ・生年月日などのプライバシー情報を含まない仮名証明書、住所や氏名等に依存しない（曖昧な記述の）識別子の導入などの検討。 法人に対する証明書発行については欧州のe-Sealの動向についても着目する必要がある。	[illegible]会でも検討が重ねられ、さらに弁護士を含む多くの構成員からこのような意見が上がってくることを重視し、署名法にとってのあるべき姿を示す時期に来ているものと思料する。 指定調査機関としての考え方は、「認定認証業務により発行された電子証明書の本来の利用方法に合わせ、属性情報の真偽確認方法についても認定の対象として明確かつ適切に規定し、法の体系を利用実態に合わせることが望ましい」とする考えに変更はない。 なお、e-Sealについては、EU規則の中で必ずしも明確となっていない部分があり、法人に対する証明書発行というもののEU委員会の考え方については、今後の慎重な検討が必要であると思料する。	現行法の枠内では対応は困難である。 来年度以降、引き続き継続して検討したい。
360O番台	<u>所属・役職，資格等の属性の記載を認証対象とすることを検討すべきである。</u> 現行の施行規則6条8号においては，氏名・住所・生年月日を除く属性は，認定の対象外である。しかし，所属・役職又は資格を示す正当な団体からの適切な文書が提出されることを前提に，認定対象たる属性の記載を認定の対象とすべきである。具体的には，所属や役職については，所属企業・法人等の文書を，資格については当該資格に係る士業団体等の証明書が考えられる。 なお，認定認証業務は，このような属性を記載した証明書を発行した場合には，その属性に係る企業・団体等に発行の旨を通知し，通知を受けた企業・団体等は，発行内容に誤りがある場合や，内容に変更が生じた場合は，ただちに失効申請を行うこととすべきである。		

項番	追加のご意見・ご質問	JIPDEC案	事務局案
3512	項番3512の規定に関連して、誤認を防止を、公開鍵の関係だけに頼っているため、様々なトラストサービス（タイムスタンプ、認証、サーバ証明書等）の信頼関係を構築できなくなっている。 マイナンバー制度導入を背景とした公的個人認証サービスの拡張では、利用者証明用電子証明書（認証用証明書）をが発行されることになる。この場合、同一の認証局から発行されるかどうかはわからないが、同一の信頼点からの、電子署名以外の用途の証明書が発行されることになると想定される。 論点としては、以下のものが考えられる。 ・認定認証業務における認証用証明書等の電子署名以外の目的の証明書の発行。 ・X.509証明書の鍵使用目的を使うことによる署名用証明書との区別を明確にする、等。 【事務局補記】 認定を受けた認証業務に係る発行者署名符号を、認定外の認証用電子証明書についても共有することはできないか、という点についても追加の質問があった。	「認証用途」の電子証明書を発行する業務は、電子署名法第2条第2項において規定される「認証業務」とは言えないため、電子署名法第4条の認定を受けることはできないとの見解が主務省から出されている。 今回もこの見解に従い、認証用証明書は認められず、署名用証明書との区別を明確にすることについても、署名法の要件外という整理でよいものと思料する。	電子署名法第2条第2項の「認証業務」と認められるためには、「電子情報の作成者を示す目的で利用者が行う電子署名」について証明する必要があり、当該電子署名の対象となる電子情報は、本人の意思で本人が作成(確認)し、本人が伝えたい意味のあるメッセージである必要がある。 本件で想定されている「認証」は、サーバがクライアントに送るデータ(乱数)に署名させ、サーバはその署名を検証して相手を認証する方式とのことなので、この場合の電子情報はサーバ側から提供されるものであり、署名する内容に意味はないと考えられる。よって、本件で想定されている「認証」は、電子署名法第2条第1項に規定する「電子署名」とは異なるものとなり、現行の電子署名法の対象とはならないと考えられる。 なお、電子署名法施行規則6条7号において、認証業務に関し、利用者等が認定認証業務と他の業務を誤認することを防止するための適切な措置を講じることとされていることを受け、電子署名法に基づく特定認証業務の認定に係る指針10条1号においては、発行者署名符号を認定認証業務以外の業務のために使用しないこととされている。 （例外として挙げられているのは、認定認証業務と同程度の基準に従って国等が実施する認証業務との相互認証の実施のための使用（同号イ）及び当該認証業務の維持管理に必要な場合における使用（同号ロ）である。）

項番	追加のご意見・ご質問	JIPDEC案	事務局案
その他Ⅰ	欧州では認証や電子署名に対してより強制力を増す流れ(eIDAS)があり、以下の議論が含まれている。 ・自然人だけでなく法人に対する証明書発行（e-Seal）に関する規定 ・認証局や電子署名サービス、電子文書配達サービスなどの信頼が必要となるサービス事業者（TSP:Trusted Service Provider）に関する規定 ・各国の認定されたTSPをリスト化し相互運用するトラストリストの整備 これらは、上記の意見に関連の強いものであり、より詳細な調査を行い、日本はこの動向にどのように向き合うか検討を行う必要がある。	左記については、EU規則の中で必ずしも明確となっていない部分が多く、今後の動向調査と慎重な検討が必要だと思料する。	これらの動向については慎重な調査と検討が必要と考える。今回はご意見を拝聴したい。
その他Ⅱ	署名法施行当時は署名ソフトをクライアントPCにインストールし署名者は私有鍵をICカードや自身のPCのハードディスク上に保管管理する運用が主であった。現在は、データセンター内に設置された自社サーバーに署名アプリを構築し、私有鍵を安全にサーバーに格納して署名運用を行ったり、クラウドサービス型の電子契約サイトや電子申請サイトに利用者の私有鍵を安全に格納して署名運用を行なうサーバ署名サービスが有用であることも多い。欧州や米国においても利用者の署名鍵を管理するサーバ署名サービスの検討が行われている。欧州においては、適格電子署名におけるサーバ署名のガイドラインなども存在する。 　日本においてもサーバ署名サービスに関する指針について、どのように整理して行く必要があるか検討が必要であると思われる。（関係者、有識者による検討の場を設置しEUの動向調査、ガイドライン等を取り纏めるなど）	左記のようなサーバー署名の技術は、安全性についての検証が現時点では不十分であると思料する。一方、2014年に公開されたEU規則には、適格電子署名ではなく、先進電子署名の要求事項として、「署名者が、本人単独の管理のもとに、高い信頼度を持って使用することができる電子署名生成データを使って作成されている」ことが規定されており、利用者の秘密鍵をサーバーに預けるような利用方法は想定していない。「適格電子署名におけるサーバ署名のガイドライン」の現行規定がどのようになっているか、EU規則の制定によりガイドラインが改定されるかどうか等について、慎重な確認作業が必要である。	サーバ署名サービスのリスクについて、十分な検討を行う必要があると考えるところ、現段階でそのような検討が尽くされているとは考えられない。

項番	追加のご意見・ご質問	JIPDEC案	事務局案
3713	長期間経過後も署名検証者が電子署名を検証可能とすべきである。電子署名法施行以降、電子申請や電子入札だけでなく民間での電子契約、電子保存等での利活用も進み電子署名付き文書が電子証明書の有効期間を超えて長期間保存されるケースも増えている。それに伴い、電子署名を長期に渡り検証可能とする長期署名技術もISOやJIS規格で標準化されてきた。一方、長期的な観点では、暗号アルゴリズムの脆弱化や認証局の廃業等の事態も想定しておく必要があり、過去に存在した暗号アルゴリズムや認証局証明書（トラストアンカの証明書）の信頼性や、過去に発行された失効情報などについて将来にわたり確認できるよう整備しておく必要がある。 　欧州のeIDASで整備が検討されているトラストリスト等を参考に日本でも過去のトラストリストを管理し公開することで、過去のトラストアンカの信頼性を検証可能にするなど、想定される課題を整理し、解決のための方策を検討する必要がある。	欧州のeIDASで整備が検討されているトラストリスト等については、今後の動向調査と慎重な検討が必要だと思料する。	長期署名技術の有効性を十分に検証する必要があると考える。今回はご意見を拝聴したい。