経済産業省委託

平成 23 年度企業･個人の情報セキュリティ対策促進事業

（電子署名・認証業務利用促進事業

（特定認証業務に関する相談業務等））

報告書

平成 24 年 3 月

一般財団法人日本情報経済社会推進協会

電子署名・認証センター

はじめに

電子署名及び認証業務に関する法律（平成 12 年法律第 102 号、以下「電子署名法」という。）は、安全かつ信頼性のある電子商取引を促進するため、電子署名が手書きの署名や押印と同等の効力のあることを規定した法律として、平成 13 年 4 月に施行された。その後、電子署名及び認証業務に係る技術およびその利用環境は絶えず進展しており、特定認証業務に関する認定制度の円滑な実施を図るためには、当該技術等の動向について、継続的に調査・研究を行う必要があるほか、特定認証業務を行う事業者や電子証明書の利用者に対して、関係する情報提供や助言等を行うことが必要である。

これらの状況をふまえ、一般財団法人日本情報経済社会推進協会「電子署名・認証センター」では経済産業省の委託を受け、電子署名および認証業務の利用促進事業に取り組んできた。

本報告書は、これまでの電子署名・認証業務利用促進事業の実績および指定調査機関としての調査実施経験等を元に平成 23 年度に実施した、電子署名法制度に基づく特定認証業務に関する相談業務等における諸活動の成果をまとめたものである。

本報告書ならびに電子署名・認証業務利用促進事業がわが国の電子署名および認証業務の一層の普及発展に寄与することを期待するものである。

平成 24 年 3 月

一般財団法人日本情報経済社会推進協会

電子署名・認証センター

－ 目　次 －

別冊 1　平成 2 3 年度(2012 年)実務者説明会資料

1. 相談窓口の設置

1.1 相談業務

特定認証業務に係る相談窓口を設け、特定認証事業者ごとに異なる設備及び業務の実施方法等を踏まえた適切な回答・助言等を遅滞なく実施した。

相談窓口は、電話、ＦＡＸ、メールなどの複数の手段を確保し、広く相談を受け付ける体制を整備することとし、委託契約締結後に遅滞なく開始し、委託契約終了日まで行った。

相談窓口を当協会の電子署名･認証センター内（4 月 1 日は東京都港区芝公園 3 丁目 5 番 8 号機械振興会館内、12 月 26 日より、移転先の東京都港区六本木一丁目 9 番 9 号六本木ファーストビル内）に設置した、

ⅰ）代表電話番号：03-5860-7571

電話による問い合わせの開設時間：

月曜日―金曜日（祝祭日および当協会が定めた日（平成 23 年 8 月 8 日～8 月 12 日、平成 23 年 12 月 29 日～平成 24 年 1 月 3 日）

開設時間帯：9:30～12:00、12:45～17:15

ⅱ）FAX:03-5573-0565

FAX による問い合わせはありませんでした。

ⅲ）電子メール：

一般の場合

Web からの問い合わせメール窓口として、電子署名･認証センターのホームページの「お問い合わせ」から、問い合わせメールによる相談窓口を設置した。

認定認証事業者の場合

別に定める個別のメールアドレスを一般の問い合わせメールとは区別して、各認定認証事業者に通知した。

ⅳ）定期報告

毎月 1 回、経済産業に対して、問い合わせ内容および回答状況について文書により、報告した。

表 1.1　定期報告状況

提出日	報告文書
2011.9.5	問い合わせ状況(4 月分)
2011.9.5	問い合わせ状況(5 月分)
2011.9.5	問い合わせ状況(6 月分)
2011.9.5	問い合わせ状況(7 月分)
2011.9.5	問い合わせ状況(8 月分)
2011.10.4	問い合わせ状況(9 月分)
2011.11.2	問い合わせ状況(10 月分)

2011.12.1	問い合わせ状況(11 月分)
2012.1.5	問い合わせ状況(12 月分)
2012.2.1	問い合わせ状況(1 月分)
2012.3.1	問い合わせ状況(2 月分)
2012.3.30	問い合わせ状況(3 月分)

電子署名･認証センター単独では回答及び助言等の実施が困難な内容又は技術的・専門的な知識を有する内容については、その問い合わせに対する調査基準の透明性を確保するため、大学教授等の外部有識者（３名）に諮問委員を委嘱し、専門的立場で問い合わせ回答内容に対する意見を聴取する体制を整備した。

諮問委員としては、

手塚　　悟　　東京工科大学コンピュータサイエンス学部 教授

早貸　淳子　　情報セキュリティ大学院大学　客員教授

宮内　　宏　　宮内宏法律事務所　弁護士

に委嘱をお願いした。

1.1.1　(1) 相談内容の分類と回答所要日数

電子署名及び認証業務に関する法律第三十三条「主務大臣は、特定認証業務に関する認定の制度の円滑な実施を図るため、電子署名及び認証業務に係る技術の評価に関する調査及び研究を行うとともに、特定認証業務を行うもの及びその利用者に対し必要な情報の提供、助言その他の援助を行うよう努めなければならない。」を受け、認定に係る認証業務の実地の調査を行っている期間における調査実施中の事業者からの相談以外に、調査中でない認定認証事業者、特定認証事業者及び一般の国民からの相談に対応し、回答を行ってきている。

なお、回答までに長時間を要したものには、同一の相談に複数の内容が含まれていた場合、質問相手と何度もやりとりを行うことが必要となった場合が殆どである。

(a)分類

相談は、内容により次の 5 種類に分類した。

① 電子署名・認証制度全般

② 認証業務のように供する設備

③ 利用者の真偽確認

④ 認証業務の実施方法

⑤ 帳簿書類の保存場所

(b) 回答所要日数(営業日)

表 1.2　回答所要日数(営業日)

分類	１日	２日	３日	４日	５日	6 日	７日	8 日	9 日	10 日以上	合計
①	44	6	3	0	0	1	0	1	0	2	57
②	1	9	6	6	15	4	25	3	1	9	79
③	0	0	1	1	0	1	1	0	1	5	10
④	1	5	5	11	10	3	12	3	4	27	81
⑤	1	3	1	2	2	0	1	0	1	5	16
合計	47	23	16	20	27	9	39	7	7	48	243

注）回答は平成 24 年 3 月 30 日現在。取下げ 1 件及び未回答 3 件は上記件数に含んでいない。

1.1.2　(2) 回答状況

回答実施までの時間は、5 営業日まで（１週間以内）のものが 133 件(約 55%)であった。昨年度は 5 営業日までものが約 70%であったが、本年度は回答所要日数が昨年度より増加した。多数の質問を同一の相談としたもの、質問相手と何度もやりとりを行うことが必要となった等により 10 日を超えるものが 48 件あった。

なお、認定認証事業者以外からの相談は、①の内容である。その数は、54 件であり、内 43 件が相談の同日に回答した。これは、認定認証事業者以外からの相談のほとんどが、電話による相談のためである。

1.1.3 (3) 問合せ対応規程

「認証業務における問合せ手続き規程」に「相談窓口業務マニュアル」をマージを実施しを行った。

また、問い合わせ内容を管理するためのデータベースとして、問合わせ管理簿を作成しており、「問合せ事業者」「受付日」「問合せ事項」「回答（完了）日」等を記録している。

1.1.4 (4) 諮問委員への問い合わせ回答内容の確認

回答及び助言等の実施が困難な内容又は技術的・専門的な知識を有する内容に該当する問い合わせがあり、諮問委員に問い合わせ回答内容に対する意見を求めるケースが１件発生した。

下記のような回答内容の確認依頼を、各諮問委員へ送付し、回答を頂いた。

（問い合わせ内容）

「施行規則第五条第二項」の解釈に関するお問合せ

ある認定認証事業者（以下「A 認証局」という。）では、利用者に発行済みの電子証明書（IC カード）の破損等の理由によって、新規の電子証明書の発行（以下「再発行」という。）が必要となった場合に、「施行規則第五条第二項」に記載されている方法により、利用者提出書類の負担の軽減と審査業務の軽減よる再発行に要する期間の短縮を目的として、新たな再発行の方式を考えています。

この方式に対する可否について ESAC にお問合せがありましたが、「施行規則第五条第二項」の解釈について A 認証局と相違が出たため、ご意見をいただきたいと存じますので、ご回答の程、よろしくお願いいたします。

１．現在の再発行の方式

現在、A 認証局で運用されている方式は次のとおりである。

利用者に発行済みの電子証明書（IC カード）の破損等の理由によって再発行の必要が発生した場合は、新規発行時と同様に利用申込書（紙）と公的書類（住民票の写し、印鑑登録証明書等）を利用者に提出頂き、認証局側でも新規発行時と同様の審査を行った後に電子証明書(IC カード)の発行を行っている。

２．新しい再発行の方式

A 認証局で考えている新しい再発行の方式では、電子証明書（IC カード）が正常に機能する時点（新規発行直後）で、利用者が予め再発行申込書への電子署名を実施して、利用者の PC 内に署名済み再発行申込書として保管しておき、IC カード破損時に当申込書を登録局宛に e メール等で提出するという方式である。具体的な手順は次のとおりである。

① 利用者は、A 認証局 WEB サイト(リポジトリ等)より再発行申込書（PDF）を取得する。
② 利用者は、Adobe Reader を利用し、発行済みの電子証明書により再発行申込書へ電子署名を行っておく。
③ IC カードが破損した利用者は、電子メール等により、登録局へ「電子署名済み再発行申込書」を送付する。
④ 登録局担当者は、Adobe Reader を利用し、再発行申込書に付与される利用者の電子署

名の有効性を検証する。

⑤ 発行局担当者は、該当する利用者の電子証明書を初回発行した際の終了期限を超えない（初回の発行可否判断日から起算して5年未満）電子証明書（ICカード）を再発行する。

⑥ 発行局担当者は、利用者へICカード及びPINを発送する。

A 認証局では本方法により、再発行時に利用者が提出すべき利用申込書（紙）や公的書類（住民票の写し、印鑑登録証明書等）の提出が省略でき、また認証局側での審査（申込書と公的書類との突合せチェック）が省略でき、電子署名の検証を行うのみで電子証明書の再発行が可能になるため、再発行に要する期間が短縮できるという認識である。

3．施行規則第五条第二項に関する解釈の相違について

施行規則第五条第二項の「現に電子証明書を有している」の解釈について、次の相違がある。

【施行規則第五条第二項】

現に電子証明書を有している利用者が当該電子証明書の発行者に対して新たな電子証明書の利用の申込みをする場合において、当該申込みに係る電子証明書の有効期間が前項に規定する方法により当該利用者の真偽の確認を行って発行された電子証明書の発行日から起算して五年を超えない日までに満了するものであるときは、同項の規定にかかわらず、当該発行者は、当該利用者が現に有している電子証明書に係る電子署名により当該利用者の真偽を確認することができる。

【ESACの解釈】

施行規則第五条第二項の「現に電子証明書を有している」とは、利用の申込みをする時点において、電子署名が可能である電子証明書を有しているものと解釈する。

したがって、A 認証局の方式では、実際に利用者が認証局に再発行の申込みをする時点で、電子証明書（ICカード）破損等によって電子署名は不可能であるので、施行規則第五条第二項に適合しない。

【A認証局の解釈】

実際に利用者が認証局に再発行の申込みをする時点では電子署名を行うことは出来ないが、申込みの時点で電子証明書は現に有効（失効されていない）であり、利用者がICカード及びPINをしっかり管理しているのに加え、ICカードが破損等によりなおさら秘密鍵の危殆化の恐れのない電子証明書を有しているので、施行規則第五条第二項に適合する。

４．お問合せ内容

次の２点について、お問合せをさせていただきます。

Ｑ１　お問合せのケースにおける「施行規則第五条第二項」の解釈について、ESAC と A 認証局のどちらを採るべきと考えられますか？ または、他の解釈が考えられるでしょうか？
ご回答：

Ｑ２　A 認証局の方式では、利用者が再発行申込書に電子署名する際には申込日を特定できないため、申込日を記入することが出来ません。この件については A 認証局も認識しており、他の方法を考えるとのことですが、この申込日についてご意見をお聞かせください。 ① 再発行申込書自体に申込日が記入されていない（または再発行申込書に申込日の欄がない）ものを、認証局として正式な再発行申込書として受理してよいのでしょうか？ ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えます。 なお、新規の利用申込書には申込日を記入させています。 ② ①で受理できないとする場合でも、再発行申込書以外の情報（例えば電子メールの送信日時等）により申込日と再発行申込書を紐づけることができれば、受理してよいのでしょうか？ ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えますが、仮に申込日と再発行申込書を紐づけてもよいとする場合には、申込日自体にも再発行申込書と同様に、改ざん防止と否認防止のために電子署名が求められるものと考えます。 ③ 再発行申込書を認証局が受理した受理日と申込日の乖離はどの程度認められるのでしょうか（例えば、1 年や 2 年等のケースを想定）？ ESAC としては、新規の利用申込書に添付する住民票の写し等の公的書類については３ヶ月以内のものを有効としていることから、同様に３ヶ月以内と考えるのが妥当だと考え

ます。
ご回答： 【①について】 【②について】 【③について】

（諮問委員からの回答内容）

a） 手塚委員

Ｑ１　お問合せのケースにおける「施行規則第五条第二項」の解釈について、ESAC と A 認証局のどちらを採るべきと考えられますか？ または、他の解釈が考えられるでしょうか？
ご回答： 結論：ESAC の解釈を採るべきと考えます。 理由：ESAC の解釈において、「施行規則第五条第二項の「現に電子証明書を有している」とは、利用の申込みをする時点において、電子署名が可能である電子証明書を有しているものと解釈する。」とありますが、この解釈を採るべきであると考えます。 一般に、電子申請処理は IC カードが正常な状態(IC カード破損等がない状態)で行われるものでありますが、電子証明書(IC カード)の施行規則第五条第二項の再発行も電子申請処理の一つであると考えられます。そうしますと、電子証明書(IC カード)の破損等の理由によって再発行を電子申請することは不可能であると解釈すべきであります。

従いまして、前もって利用者の署名付き再発行申込書を使って電子申請をすることは、認めることはできないと考えます。

Ｑ２　A 認証局の方式では、利用者が再発行申込書に電子署名する際には申込日を特定できないため、申込日を記入することが出来ません。この件については A 認証局も認識しており、他の方法を考えるとのことですが、この申込日についてご意見をお聞かせください。

① 再発行申込書自体に申込日が記入されていない（または再発行申込書に申込日の欄がない）ものを、認証局として正式な再発行申込書として受理してよいのでしょうか？
ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えます。
なお、新規の利用申込書には申込日を記入させています。

② ①で受理できないとする場合でも、再発行申込書以外の情報（例えば電子メールの送信日時等）により申込日と再発行申込書を紐づけることができれば、受理してよいのでしょうか？
ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えますが、仮に申込日と再発行申込書を紐づけてもよいとする場合には、申込日自体にも再発行申込書と同様に、改ざん防止と否認防止のために電子署名が求められるものと考えます。

③ 再発行申込書を認証局が受理した受理日と申込日の乖離はどの程度認められるのでしょうか（例えば、1 年や 2 年等のケースを想定）？
ESAC としては、新規の利用申込書に添付する住民票の写し等の公的書類については３ヶ月以内のものを有効としていることから、同様に３ヶ月以内と考えるのが妥当だと考えます。

ご回答：

【①「　ついて】

申込日の記入は必須であると思いますので、申込日の記載がない再発行申込書は受理すべきでないと考えます。

従いまして、前もって申込日を特定できない利用者の署名付き再発行申込書を使って電子申請することは、不可能になります。

【②について】

再発行申込書の電子申請は、あくまでも利用者本人の意思に基づくものでないといけないと考えますので、単に申込日と再発行申込書が技術的に紐づけば良いというわけではないと考えま

す。
　従いまして、改ざん防止はもちろんのこと、否認防止の対策が施されている必要があり、この意味からも利用者(再発行申込者)の電子署名が必要であると考えます。

【③について】
受理日と申込日の乖離は、本来は電子証明書(IC カード)の破損等が発生した場合には、速やかに対応する必要があると考えますが、具体的には、ESAC が提案しております考え方の 3 カ月以内が妥当であると考えます。

b) 早貸委員

Ｑ１　お問合せのケースにおける「施行規則第五条第二項」の解釈について、ESAC と A 認証局のどちらを採るべきと考えられますか？
　または、他の解釈が考えられるでしょうか？

ご回答：
　施行規則第五条第二項に適合しないと考えます。申込みをする時点において、有効な電子証明書に係る電子署名を行うことができることが必要であると考えます。

　ちなみに、本件 A 認証局の考え方に立つと、IC カードが破損した以後の日付をもって他人がした電子署名（できてしまった理由については、鍵の漏えい等いろいろあり得るとは思いますが。）について、その電子署名は本人がしたものではないことを抗弁する場合には、電子証明書の失効等も予定されていないところ（というか電子証明書は有効であると言う前提だとすると)、「IC カードがいついつから破損していたので、電子署名はできなかったんです」ということを別途立証するということになるんですかね？

Ｑ２　A 認証局の方式では、利用者が再発行申込書に電子署名する際には申込日を特定できないため、申込日を記入することが出来ません。この件については A 認証局も認識しており、他の方法を考えるとのことですが、この申込日についてご意見をお聞かせください。

① 再発行申込書自体に申込日が記入されていない（または再発行申込書に申込日の欄がない）ものを、認証局として正式な再発行申込書として受理してよいのでしょうか？
　ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えます。
　なお、新規の利用申込書には申込日を記入させています。

② ①で受理できないとする場合でも、再発行申込書以外の情報（例えば電子メールの送信

日時等）により申込日と再発行申込書を紐づけることができれば、受理してよいのでしょうか？

ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えますが、仮に申込日と再発行申込書を紐づけてもよいとする場合には、申込日自体にも再発行申込書と同様に、改ざん防止と否認防止のために電子署名が求められるものと考えます。

③ 再発行申込書を認証局が受理した受理日と申込日の乖離はどの程度認められるのでしょうか（例えば、1 年や 2 年等のケースを想定）？

ESAC としては、新規の利用申込書に添付する住民票の写し等の公的書類については３ヶ月以内のものを有効としていることから、同様に３ヶ月以内と考えるのが妥当だと考えます。

ご回答：

【①について】

いつの時点における署名者の意思が表象されているのかが特定できないと推定効には結び付けづらいところ、電子署名認証業法が規定する特定認証業務については、いつの時点における電子署名であるかを技術的に担保する要素はとりこまれていないこともあり、申込日は必要である（その時点における意思が表象されていると考えるとの整理）と考えます。

【②について】

電子署名をした者の意思が表象されているとの推定が働く対象は、電子署名が付されたデータであって、そのデータが点々と流通した場合であっても、電子署名によりデータ作成時における署名者の意思の表象であるという推定が働くと言う前提で考えると、封筒の中に文書の作成年月日の問題と、封筒の消印の問題は紐づけられないのと同様に、紐づけは困難ではないかと考えます。電子メールの送信日時に紐づけられるのは、メール本文等の記載事項のみだと思いますので。

【③について】

一般論として、期限の定め（〇〇を紛失した場合には、〇日以内に･･･等）があるものでなければ、原因となる事実が発生してから申込みまでの期間や、申込書を作成してから実際に提出するまでの期間には制限がないと言わざるを得ないかもしれませんが、本人の申込み意思の確認手段として位置づければ、署名されてから 3 月以内とのセンターの考え方は妥当であろうと思料します。

本件についていえば、まだ申込み意思が発生していなかった時点で作成された申込書であるとの前提が示されている以上、その時点の申込みも意思表示として有効であるとは言えないと言わざるをえません。

意思表示の時点において、表示に係る意思がなかったことを知りながら、有効な意思表示と

して扱うと、民法上の虚偽表示か、心裡留保における相手方が事情を知っていた場合に該当して、いずれにしても意思の欠缺（ケンケツ）により無効となってしまいそうな気がします。

意思表示として成立させるための解決の方法としては、IC カードの破損等を停止条件とする条件付きの再発行の申込みの意思表示と位置付け、IC カードの破損の事実を停止条件の成就として別途報告するみたいな方法もあるかもしれませんが、そうすると、現時点において電子証明書で検証できる電子署名ができないことを明らかにしてする申し込みになるので、やはり形式的に施行規則第五条第二項に適合しないと考えます。

c） 宮内委員

Ｑ１　お問合せのケースにおける「施行規則第五条第二項」の解釈について、ESAC と A 認証局のどちらを採るべきと考えられますか？
または、他の解釈が考えられるでしょうか？

回答：

第 5 条 2 項の「現に電子証明書を有している」の部分については，A 認証局の解釈になると思います。その理由は以下のとおりです。

理由１： リボークされていない以上，文言上は，電子証明書自体は有効と思われます（有効でないとする理由に乏しいと思います)。なお，IC カード破損時には証明書を失効させるべきですが，本人から失効の申請がない限り，失効はしていないと考えます。

理由２： 仮に，有効な証明書・有効なカードを有している利用者が，継続等のなんらかの理由で再発行の申請を行ったとします。その利用者が申請を作成後，申請が受け付けられる前（あるいは利用者の真偽を確認する前）にカードを壊したケースを考えます。これは，申請を受け付けるべきだと考えます。このとき，同項後半の「現に有している電子証明書に係る電子署名により当該利用者の真偽を確認する」にあたって，確認の時点でも「現に有している」と言えるためには，A 認証局の解釈を取るしかありません。

Ｑ２　A 認証局の方式では、利用者が再発行申込書に電子署名する際には申込日を特定できないため、申込日を記入することが出来ません。この件については A 認証局も認識しており、他の方法を考えるとのことですが、この申込日についてご意見をお聞かせください。

① 再発行申込書自体に申込日が記入されていない（または再発行申込書に申込日の欄がない）ものを、認証局として正式な再発行申込書として受理してよいのでしょうか？
ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えます。
なお、新規の利用申込書には申込日を記入させています。

② ①で受理できないとする場合でも、再発行申込書以外の情報（例えば電子メールの送信日時等）により申込日と再発行申込書を紐づけることができれば、受理してよいのでしょうか？

ESAC としては、再発行申込書自体に申込日を記入させるべきであると考えますが、仮に申込日と再発行申込書を紐づけてもよいとする場合には、申込日自体にも再発行申込書と同様に、改ざん防止と否認防止のために電子署名が求められるものと考えます。

③ 再発行申込書を認証局が受理した受理日と申込日の乖離はどの程度認められるのでしょうか（例えば、1 年や 2 年等のケースを想定）？

ESAC としては、新規の利用申込書に添付する住民票の写し等の公的書類については３ヶ月以内のものを有効としていることから、同様に３ヶ月以内と考えるのが妥当だと考えます。

回答：

【①について】

これは，申請時の意思表示を確認するものにはならないと考えます。

署名済みの申請書は，署名を行ったとき（それがいつだかわからない）の意思を示すものではありますが，申請時の意思表示を確認することにはならないからです。

したがって，申請時の意思が不明ですから，受理すべきではないと考えます。

【②について】

署名付の申請書に加えて，申請時の意思を確認する必要があるわけですが，そのためには，それなりの本人認証が必要です。電子メールを出してきただけでは，申請時点での本人の意思の確認としては不十分であると考えます。第 5 条 1 項 1 号本文の本人確認までは不要だとしても，「それなり」の確認が必要と思います。

「それなり」の確認をどうするか，と言うのが問題となります。私見ですが，例えば，第 5 条 1 項 1 号但書きに規定される代理人の認証の規定を準じて考えてはどうか，と思います。つまり，本人が出した申請書ではあるものの（これが委任状相当），申請時点での本人の意思が確認できないので，1 号イ～ハのいずれかのもので申請時点での本人の意思表示であることを確認すると言う考え方です。

【③について】

３ヶ月以内，という意見に賛成します。

2. 問い合わせに関する Q&A の整備

相談者に対し、的確かつ迅速に回答できるよう、平成 19 年度以降の本事業の委託期間に、相談窓口に寄せられた問い合わせ（守秘義務に係る問い合わせを除く）、それらに対する回答をまとめ Q&A を作成した。

2.1 一般からの問い合わせ Q&A

一般からの問い合わせは全て問い合わせ分類の①電子署名･認証制度全般である。

1. 電子証明書について		
No.	相談内容	回答内容
1	電子証明書の入手方法を教えて下さい。	認定認証事業者から電子証明書を入手する方法は認証業務ごとに差異があり、事業者のホームページ（下記①を参照）に掲載されているので、それをご参照ください。なお、一般的な手順は下記のとおりです。 ①使用目的に合った電子証明書を発行している認定認証業務(認証局）を選択する 認定認証業務一覧は、下記サイトを参照してください。 法務省 （http://www.moj.go.jp/MINJI/minji32.html） 経済産業省 （http://www.meti.go.jp/policy/netsecurity/esig-srvlist.html） ②利用申請書及び申請に必要な書類を準備する（多くの場合、住民票の写し及び印鑑登録証明書等が必要。外国籍の方は、住民票の写しに代わり登録原票記載事項証明書が必要。） ③利用申請書を作成し、申請に必要な書類と共に認証局に郵送する ④認証局で利用申請書を審査し、審査が通れば、認証局から電子証明書を格納された媒体が郵送されてくる（あるいは電子証明書をダウンロードするための情報が送られてくる）

		⑤電子証明書を受領したら、電子証明書の記載内容を確認の上、認証局に受領書（③の申請時に使用した印鑑で押印あるいは発行された電子証明書で電子署名）したものを郵送（あるいはメール送信）する
2	電子証明書を取得するまでの期間はどのくらい必要でしょうか？	電子証明書を発行する認証業務を行っている認証事業者によって電子証明書を取得するまでの期間は異なっております。通常の発行状況では、おおむね2週間から1カ月くらいが目安になると思われます。 具体的な期間をお知りになりたい場合には、利用したいと思う認証事業者に個別に問い合わせて下さい。また、電子証明書には認証事業者毎に、使用用途が決められておりますので、使用用途に合わせて認証事業者をお選びください。
3	認定認証業務が発行する電子証明書は個人にしか発行されないのでしょうか？	電子署名法で認定している認定認証事業者が発行する電子証明書の対象は自然人に限定されています。
4	法人に発行される電子証明書はないのでしょうか？	認定認証業務で発行する電子証明書は自然人を対象としており、法人には発行できませんが、法人登記の情報を基に、法務省登記所で発行される「商業登記に基づく電子認証制度（http://www.moj.go.jp/ONLINE/CERTIFICATION/index.html）」では、法人の代表者に対する電子証明書が取得可能です。このほか、民間の認証事業者〔認定認証業務以外〕でも法人に電子証明書を発行しているものがあります。
5	電子証明書は有料でしょうか？	一般的には、認定認証業務で発行している電子証明書は有料です。電子証明書には有効期間があり、有効期間によって価格が異なっております。概ね、1年間有効の電子証明書の価格は1万円程度です。
6	電子文書に電子署名するごとに課金されるのでしょうか？	一般的には、電子文書に電子署名する時に必要な電子証明書を、認証局から取得する際に（有効期間により価格が異なる）費用が発生します。電子文書に

		電子証明書で電子署名するごとには課金されません。
7	利用者の秘密鍵と公開鍵はどこで作成されるのでしょうか？	電子証明書を発行する認証業務を行っている認証局で利用者の秘密鍵と公開鍵を作成するケースと、利用者側で秘密鍵と公開鍵を作成するケースがあります。 認定認証業務では、認証局側で作成するケースが一般的です。
2. 電子署名の概念や仕組みについて		
No.	相談内容	回答内容
1	電子署名の概念や仕組みについて教えて下さい。	電子署名・認証センターのホームページ（http://www.jipdec.or.jp/esac/index.html）上で電子署名について（電子署名の必要性、電子署名の仕組み、電子署名と認証業務、電子署名における義務と責任および電子署名法の解説）掲載しておりますので、ご参照下さい。 なお当該ホームページは、経済産業省委託事業「電子署名・認証業務利用促進事業」の一環として作成されたものです。
2	電子署名に関するセミナー等について教えて下さい。	電子署名の方法や仕組み等に関して、有料あるいは無料のセミナーがあります。有料の場合は、セミナー等を行っている研修機関等で PKI、電子署名等のキーワードで検索されると情報が見つけられると思います。 無料のセミナーとしては、毎年、経済産業省が電子署名・認証業務利用促進事業として電子署名・認証業務普及セミナー、タイムビジネス協議会がタイムビジネスシンポジウム（http://www.dekyo.or.jp/tbf/seminar/index.html）、社団法人日本画像情報マネジメント協会（JIIMA）が e-文書に関わるセミナー（http://www.jiima.or.jp/）及び NPO 日本ネットワークセキュリティ協会（JNSA）（http://www.jnsa.org/）が PKI Day（PKI 相互運

		用技術 WG 主催セミナー）等を開催しております。 　また、認証業務を行っている事業者に於いてもセミナー等を無料で開催していることがあります。 　電子署名・認証業務普及セミナーにつきましては、電子署名・認証センターのホームページ（ http://www.jipdec.or.jp/esac/promotion/index.html）に過去のセミナーの講演内容を紹介しておりますので、ご参照ください。
3	電子署名の用語解説として、電子署名とデジタル署名のどちらを用いた方がよいのでしょうか？	電子文書に対する署名には、デジタル署名（Digital Signature）と電子署名(Electronic Signature)の２つの用語が用いられています。 電子署名とは、電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電子的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適切に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。（電子署名法第三条） 一方、デジタル署名は、公開鍵暗号方式（PKI)を利用したもので、電子文書の発信者の認証と改ざんの検知が可能です。 一方、電子署名は、デジタル署名を含む広義の署名として用いられ、電子データの作成者を特定でき、電子データが改変されていないことが確認できます。 国の認定認証業務で発行される電子証明書は PKI を利用するものですが、電子署名を用いています。
3.　電子署名について		
No.	相談内容	回答内容
1	電子署名で何ができるののでしょうか？	電子署名とは、電子情報の発信主体が本人であること（なりすまし防止)、また、発信されたデータが改ざんされたものでないことを証明するために用いられます。 電子入札などでは提出する入札書の電子ファイル

		に電子署名することが求められることがあります。入札者が入札資格を持つ本人によって作成され、かつ、金額などの内容が改ざんされていないことを証明するために、認定認証業務が発行する電子証明書を使用して、電子署名します。また、契約書等を電子文書で行う場合についても、電子証明書を使用して契約書（電子文書）に電子署名する時に使用します。 詳細は電子署名･認証センターのホームページもご参照ください。 （ http://www.jipdec.or.jp/esac/example/jirei.html）
2	電子文書へ電子署名することが可能な具体的なソフトウェアを教えて下さい。	電子文書を作成するソフトウェア（例えば、Microsoft® Word®、Microsoft® Excel®、Microsoft® PowerPoint®、電子メールクライアント（Microsoft® Outlook®、オンラインサービスである Windows Live™メール、Thunderbird®等））では、多くの場合電子証明書で電子署名する機能を持っています。電子入札用のクライアントソフトウェアは、一般的に電子証明書を販売している認証局から配布されています。詳細については、具体的に利用する用途に対応した電子証明書を発行している認証事業者に問い合わせて下さい。 ※ Microsoft® Word® 、 Microsoft® Excel® 、 Microsoft® PowerPoint®、Microsoft® Outlook®、Windows Live™ メールは、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。以下、同じ。 ※Thunderbird®は、米国 Mozilla Foundation の米国及びその他の国における商標または登録商標です。以下、同じ。
3	電子メールを送信する際に、電子署名を付ける方法について教えて下さい。	電子証明書を使った電子メール送受信を簡単に説明すると、 ①電子証明書を入手（電子メールに電子署名できるもの） ②電子メールクライアント（例としては、

		Microsoft® Outlook®、Windows Live™メール、Thunderbird®及び Shuriken 等）に使用する電子証明書をインストール ③電子メールを送信する時に、その電子メールにインストールした電子証明書で電子署名し、送信する ④電子メールを受信したときの確認方法につきましては、Microsoft® Outlook®を例とした手順が次の URL にありますので、参考にしてください。 （http://www.jipdec.or.jp/esac/example/index.html） また、電子証明書インストールガイド （ http://www.jipdec.or.jp/project/anshinkan/jcan/install.html）などもご参照ください。 ※「Shuriken」は、株式会社ジャストシステムの登録商標です。
4	電子署名付きの電子メールを読むために、何か追加でインストールする必要がありますか？	電子署名の内容が有効であるかを確認し、発信者が信頼できる（なりすましされていない）か検証するためには、以下の 2 点にご注意いただく必要がございます。 ①パブリック電子証明書を利用する場合 一般的に使用されているメールソフト（例えば、Microsoft® Outlook®、Windows Live™メール、Thunderbird®等）では、専用のソフトウェアのインストールを必要とせずに、電子メールに電子署名された電子証明書を検証することができます。 ②パブリックでない、組織独自の電子証明書を利用する場合 電子証明書発行元の信頼性を確認した上で、専用のソフトウェアをインストールする、あるいは当該電子証明書を検証するために必要なルート証明書等をインストールする必要があります。 詳細につきましては、各電子証明書の発行元にお問い合わせください。また次の URL 等を参考にしてく

		ださい。 （http://www.jipdec.or.jp/esac/intro/gaiyou.html#tyuui02） なお、電子署名付きのメールの電子署名を検証せずにその文面を読むことは可能です。この場合、何かを追加でインストールする必要はありません。 注）パブリックとは Windows OS やメールソフトの証明書ストアに、電子証明書を発行した認証局のルート証明書が格納されているもの
5	電子署名を付けた電子メールを外国の人でも検証することは可能でしょうか？	日本で取得した電子証明書を外国人が検証することは可能です。 なお、検証する電子証明書に記載される属性情報として日本語の部分がある場合には、当該属性情報の閲覧に日本語対応するソフトウェアが必要になります。
6	電子文書(請求書等）へ電子印を押す（電子署名する）ことの有効性について教えて下さい。	電子印は一般的に印刷（表示）等をした場合、あたかも印鑑による押印があるように見せるものです。また、電子情報の発信主体が本人であること（なりすまし防止)、発信されたデータが改ざんされたものでないことを証明するためのものとして電子署名があります。電子印の中には、押印する際に、押印と共に電子証明書で電子署名を付与するシステムがあります。 押印と共に電子証明書で電子文書に電子署名した場合、電子署名された電子文書（この場合は請求書）は、法的に真正に成立したものと推定されます（電子署名法第三条)。 電子証明書の機能等については、当協会のホームページを参照してください（http://www.jipdec.or.jp/esac/intro/index.html）
4.　電子署名を使用したアプリケーションについて		

No.	相談内容	回答内容
1	電子文書(契約書､注文請書等)の場合は印紙税がかからないのでしょうか？	電子文書の場合は印紙税不課税となる事例がありますが、お問い合わせのケースについては所管税務当局にご確認ください。 【参考：印紙税不課税】印紙税については、電磁的記録により作成されたものについて課税されないことが、「国会答弁書第九号内閣参質一六二台九号（平成十七年三月十五日）」及び「税務通信2001.5.14」等で確認されています。
2	株主総会等の議事録の承認に電子署名を利用し、インターネットを介して行う場合は、電子証明書の導入に係る費用はどのくらいでしょうか？	一般的には、1 年間有効の電子証明書は 1 枚 1 万円程度で購入することができます。IC カードタイプの電子証明書を使用する場合、IC カードの読み取り装置（IC カードリーダ等）が必要となる場合があります。
3	利用者とインターネットを介し、タブレット PC で手書きサインを使用してオンライン契約をすることは可能でしょうか？	タブレット PC の画面での手書きサインは、画像情報であり改ざんが可能であること、画像情報では手書きサインをした個人を特定する情報が含まれないことから、画像情報そのものでは、電子署名としては認められません。 オンライン契約(電子契約)には、契約の主体である双方の電子署名を付した契約情報が必要となります。電子署名を付すためには各利用者が電子署名に対応した電子証明書を所持している必要があります。
4	電子文書の長期保存に係るタイムスタンプとしてはどのようなものを利用すればよいのでしょうか？	電子文書の長期保存では、文書に作成者(作成責任者)の電子署名を付与し、その後、この電子署名に対応する電子証明書に係る失効情報、発行局の情報(失効情報を含む)等を添付し、これにタイムスタンプを付与して、安全に保存することが必要です。 使用するタイムスタンプは、法律的規制はありませんが、(財)日本データ通信協会が行っているタイムビジネス信頼・安心認定制度の認定を取得しているものがありますので、(財)日本データ通信協会のホームページ（http://www.dekyo.or.jp/）を確認

		して下さい。
5	e-Gov 電子申請システムで使用可能な電子証明書を発行している認証局を教えて下さい。e-Gov 電子申請システムで使用可能な電子証明書を発行している認証局を教えて下さい。	電子政府の総合窓口(e-Gov：イーガブ)で電子申請する場合、電子署名が必要な場合があります。「申請者の電子証明書を発行する認証局」が下記 URL にありますので、参照してください。 （http://shinsei.e-gov.go.jp/menu/setup/manu_certificate.html）
6	どのようにしたら電子定款オンライン申請ができるのでしょうか？	会社設立に係る登記申請するには、個人ですべてを実施する方法と、司法書士を利用する方法があります。個人で実施する場合は、電子定款オンライン申請システムで利用できる電子証明書を取得する必要があります。 また、電子定款申請等に関する情報が、法務省の登記所のページ（http://www.touki-kyoutaku-net.moj.go.jp/）及び日本司法書士会連合会のホームページ（http://www.shiho-shoshi.or.jp/）にありますので、そちらを参照して下さい。
7	電子定款オンライン申請を行政書士等の資格のないものが代理人申請できますか？	法務省の電子定款オンライン申請（現在は、登記・供託オンライン申請システム）では、代理人として行政書士を前提としていますが、詳細については法務省の担当部門（民事局 http://www.moj.go.jp/MINJI/index.html）にご確認下さい。
8	外部とネットワーク接続していないところで電子文書へタイムスタンプを付与することができますか？	電子文書へ付与するタイムスタンプは、日本標準時に同期した時刻源（Time Authority）から時刻情報を提供されたタイムスタンプ認証局(Time Stamping Authority）が発行する必要があり、外部ネットワークから独立したネットワークで構成されたところで電子文書を作成する場合、当該ネットワーク内に時刻源とタイムスタンプ認証局を設置する必要が発生します。

9	電子契約(雇用契約)を、海外の契約者と行うことは可能でしょうか？	雇用契約の契約書を電子契約書として取り結ぶことは可能であると思われます。契約書には契約を結ぶ両者が電子署名することになります。契約相手が海外の会社の場合は、相手先の国が電子契約を認めているか、あるいは、電子契約に係る法律があり、その条件を満たすことができるか等について、個々の国ごとに確認する必要があります。（例えば、その国が認める電子証明書発行者である必要がある、認証業務の真偽確認方法等について規制がある等が考えられる。また、相互承認をしている場合は、その条件を確認する必要がある。）

5. 電子署名法の解説

No.	相談内容	回答内容
1	一般の認証業務、特定認証業務、認定認証業務の差異について教えて下さい。	電子署名法では、「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務です。（法第二条第二項） 特定認証業務とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして、主務省令（「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わる指針」等）で示す基準に適合するものについて行われる認証業務です。（法第二条第三項） 特定認証業務で、主務省（総務省、法務省、経済産業省）の認定を受けたものが認定認証業務です。（法第四条第一項）
2	認定認証業務を始めるにはどのくらいの費用と期間が必要でしょうか？	新規に認証業務を構築し、特定認証業務の認定を取得する場合、認証局の構成、規模等により構築に係る費用や調査費用は変動し、一律いくらという料金ではないため、明確に回答することはできません。 また、認定を取得し、継続して認定認証業務を実施する場合は、「電子署名及び認証業務に関する法律」（電子署名法）の規定により、１年ごとに認定を更

		新する必要があり、このため、認定更新に係る調査を毎年受ける必要があります。 認定の更新を行う場合の認定更新調査に係る調査料金は過去の実績ではおおよそ 1 年目の認定更新時は 400 万円程度となります。2 年目以降は、300 万円程度となります。調査手数料の詳細については、以下の URL を参照して下さい。 http://www.jipdec.or.jp/esac/agency/pdf/fee_2.pdf 指定調査機関による調査に係る調査料金以外にも、電子署名法で義務づけられている準拠性監査を認定の更新前までに、毎年実施する必要があり、経費が発生します。その他、利用者対応の窓口の維持等の運営経費も必要となります。また、認証局の施設や設備の維持管理に係る費用も発生します。 新規認定を取得するまでの手順は、電子署名･認証センターの HP に掲載されています「認定に係る調査手順（http://www.jipdec.or.jp/esac/agency/pdf/jipdectejyun.pdf)」を参照してください。また、「特定認証業務の認定に係る調査表（http://www.jipdec.or.jp/esac/agency/dl-chosa.html)」を元に認定に係る調査を実施いたします。新規認定の場合、調査表の調査項目について新規認定を取得しようとする事業者からのご相談から新規認定申請まで、約半年から 1 年くらい必要となります。
3	認定認証業務を行うための要件を教えて下さい。	認定認証業務を実施するために必要となる認定の取得及び認定取得のために必要な認証業務用設備及び認証業務用設備室に係る要件、運用要件等については、「電子署名及び認証業務に関する法律施行規則」、「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」、及び「電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針」に具体的に規定されています。電子署名法第六条第一項第一号から第三号に規定されたいずれにも適合していると認められなけ

		れば、認定を受けることができません。これらの法律は、e-Gov のホームページ（http://www.e-gov.go.jp/）や ESAC ホームページに掲載された法令集（http://www.jipdec.or.jp/esac/promotion/pdf/horei.pdf）で確認可能です。 認定の申請を受けて、これらの要件を調査するために調査表が公開されています。（http://www.jipdec.or.jp/esac/agency/dl-chosa.html）
4	電磁的記録の真正な成立の推定について教えて下さい。	電子署名法第三条では、「電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電子的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。」と規定されています。 この要件を満たす電子署名が行われた電磁的記録は、自筆署名や押印が行われた文書（紙媒体）と同様に、真正に成立したものと推定されることになります。
6. 電子署名･認証センターについて		
No.	相談内容	回答内容
1	電子証明書を発行していますか？	電子署名・認証センターは、指定調査機関として電子署名法の認定に関する調査を実施する機関であり、電子証明書は発行しておりません
2	電子署名･認証センターのホームページに掲載されている情報を利用することはできますか？	電子署名･認証センターのホームページに掲載されているデータを利用する場合は、以下の条件でご利用ください。 利用条件 （1）データ（図を含む）は、修正せずにそのまま使用すること。 （2）各データ（図を含む）には、出典を明記すること。
3	認定認証業務が認定を受けている旨の表示を製品パンフレット等に使用	電子署名法第十三条第一項では、「認定に係る業務の用に供する電子証明書等に、当該業務が認定を受

	することができますか？	けている旨の表示を付すことができる。」としております。また、同条第二項では、「何人も、第一項に規定する場合を除くほか、同項の表示又はこれと紛らわしい表示を付してはならない。」としており、認定を受けた認証業務に係るもの以外の他の認証業務に係るもの、または認定認証事業者でない者が当該表示を行なってはならないこととされております。また、これらに違反した場合については、電子署名法第四十二条に罰則が規定されております。 　また、当該表示は法律で規定されているものであり、電子署名・認証センターでは電子署名法の主務省から特別に許可をいただき、認定認証業務のみが使用可能なマークとしてホームページ上に掲載しております。 （http://www.jipdec.or.jp/esac/company.html）
4	電子署名･認証業務に関する統計情報はどこにありますか？	認証事業の実態の全容が捉えられていないので、一般的な統計情報は存在していません。 認定認証業務については、総務省、法務省、経済産業省が電子証明書の発行枚数、有効枚数等を把握しております。問い合わせ先としては、総務省(情報セキュリティ対策室)または、経済産業省(情報セキュリティ政策室)となります。 認定認証業務による電子証明書の発行枚数に関しては、総務省からデータの提供を受けて、電子署名･認証センターのホームページに掲載しています。 （http://www.jipdec.or.jp/esac/agency/index.html）
5	指定調査機関とはどのような業務を行うところか教えて下さい。	一般財団法人日本情報経済社会推進協会（旧：(財)日本情報処理開発協会）は、平成 15 年 4 月に指定調査機関としての指定を受け、電子署名・認証センターが特定認証業務の調査を実施しています。特定認証業務を行う事業者が、主務大臣の認定を受けようとする場合、業務の実施に係る体制について調査を受ける必要があります。調査は、認定調査・更新調査・変更調査の 3 種類の調査があります。

6	電子署名を使用したアプリケーションの構築に関して教え下さい。	電子署名を使用したアプリケーションの構築等に関するコンサルタント業務は実施しないこととしています。
7	認定認証業務の年度ごとの電子証明書発行枚数は、いつ頃更新されるのでしょうか？	毎年 6 月初旬頃に総務省からデータを入手し、ホームページを更新しています。
8	認定認証業務の自己署名証明書、または、ルート証明書は、IE の証明書ストアにルート証明書として登録されていますか？	現行認定認証業務の自己署名証明書が IE の証明書ストアにルート証明書として登録されている事実はありません。

2.2　認定認証事業者からの問い合わせ Q&A

2.1.1　2.2.1 認定認証事業者からの問い合わせ Q&A（電子署名･認証制度全般編）

この問い合わせ Q&A は、問い合わせ分類①の電子署名･認証制度全般についてまとめたものです。

1. 電子署名･認証制度全般		
No.	相談内容	回答内容
1	認証局が利用者署名符号を管理することは問題ないでしょうか？また、認証局以外で利用者署名符号を管理することは問題ないでしょうか？	利用者署名符号を認定認証事業者が作成する場合であって、かつ、当該署名符号を認定認証業務が預託のために管理することは、施行規則第六条第三号の観点から、認められないと考えます。 また、利用者に渡された利用者署名符号の管理については、電子署名法第三条に「本人による電子署名（これを行うために必要な符号及び物件を適切に管理することにより、本人だけが行うことができることとなるものに限る。）」と規定されていることから、利用者署名符号は適切に管理され、第三者が容易に当該署名符号により電子署名できないようになっている必要があります。また電子署名法に基づく特定認証業務の認定に係る指針第八条に基づき、「電子署名は自署や押印に相当する法的効果が認められ得るものであるため、利用者署名符号については、十分な注意をもって管理する必要があること」について、利用申込者に対する説明責任があります。
2	出入国管理・難民認定法改正案について改定がありましたが、外国籍の方向け証明書発行時の真偽確認に影響があるものと考えていますが、どのような影響があるのか教えて下さい。	法律の改正に伴って、関連法規が改正されることとなります。その場合、電子署名法にも影響があれば施行規則が改正されることとなりますので、その時期に、皆様に対応方法等についてご連絡できるものと考えています。 （追記） 現行の外国人登録制度を廃止し、法務大臣が適法に在留する外国人に対して空港等で在留カードを発行する「出入国管理及び難民認定法及び日本国との平和条約に基づき日本の国籍を離脱した者等の出入国管理に関する特例法の一部を改正する等の法律」が第171 回国会で成立し、平成21 年7 月15 日に公布されています。

3	指定調査機関が、主務三省に提出している更新調査に関する調査報告書を開示いただくことは可能でしょうか？	電子署名法第二十三条にあるとおり、指定調査機関の役員若しくは職員又はこれらの職にあった者は、調査の業務に関して知り得た秘密を漏らすことはできません。調査報告書を開示することは同条違反となり、法第四十二条第二号が適用され、一年以下の懲役又は百万円以下の罰金に処せられます。
4	実地調査時だけ、実際に業務を行う要員以外が実施しても問題ないでしょうか？	業務を行うことが可能な最低人数は揃えて調査を受けてください。認定に係る調査では、施設、設備、システム及び業務の運用手続きを確認するとともに、電子署名法施行規則第六条第十五号ホの要件、つまり、「業務に係る技術に関し充分な知識及び経験を有する者の配置」が行われることが求められます。 認定を受けようとする特定認証業務の要員における充分な知識、技術の習熟度を確認するため実地調査では、調査員が、実際のオペレータ等に想定されるケースについて対応方法の質問や、模擬対応を求めることがあります。従って、実際の操作員でない方、例えば部外者やコンサルタントの方が実地調査を受けることはできません。
5	当認証局が発行した利用者電子証明書をSSL通信時のクライアント認証に使用することが可能でしょうか？	当該認定認証業務から発行された利用者署名符号及び電子証明書のSSL 通信時のクライアント認証における使用可否については、認定認証業務の利用者署名符号を電子署名以外の用途に用いることに関して、認定認証業務の利用者の便宜を図るために、認定認証事業者が当該業務の利用者に限定して個別に提供する通信サービスにおいて、当該認定認証業務に係る電子証明書をSSL 通信に使うことは可能です。 実施に際しましては、利用者サービス及び電子証明書の確認において、利用者署名符号並びに電子証明書が電子署名以外の用途で利用されることをCP/CPS等に明確に規定し、利用者の署名符号を用いて電子署名が為される際あるいは電子証明書を通信相手等に提示させる際には、事前に確認のメッセージを利用者に明示する必要があります。クライアント認証に使用する方法の詳細については、個別に指定調査機関までお問い合わせください。
6	認定認証局から発行された電子証	当該認証局の電子証明書の利用目的に合致している

	明書を契約関係書類の電子文書長期保管システムで使用することは問題ないでしょうか？ ＜添付資料＞ 説明資料	場合においては、請書、契約書等、電子商取引に係る文書等に、利用者署名符号によって署名をすることは、何ら問題はないものと考えます。 契約関係書類の長期保存サービスにおける電子証明書の利用については、当該認証業務の運用規程（CP/CPS）に電子文書保存サービスへの適用を明示的に規定される方が、利用者等の理解を得やすいように思います。 また、アーカイブタイムスタンプ付与時に、利用者(のシステム)が当該認証局の公開しているCRL 等を取得して署名検証を実施後に、これをXAdES 形式のデータの中に組み込むことは、通常のCRL 等の利用であると考えられることから特段の問題はないと思料します。 さらに、認証局の発行者電子証明書、ARL についてもCRL の場合と同様と考えられることから、これらの取得、並びに、XAdES 形式のデータの中に組み込むことは、特段の問題はないと考えます。
7	利用者に発行済みの電子証明書の電子署名により利用者の真偽の確認を行うこと（施行規則 第五条第二項）が認められていますが、この方法により発行する電子証明書に指定できる有効期間は、どうなりますか？ ① ５年を超えない有効期間であれば発行できる（施行規則第六条第四号） ② 初回に発行した証明書の発行日から起算して５年を超えない有効期間 （初回に発行した証明書の有効期限を超えることは出来ない） 施行規則の規定では、②であると考えていますが、認識に誤りがないか、念のため確認させていただくものです。 (図 1.1 を参照)	施行規則第五条第二項にあるとおり、「当該利用者の真偽の確認を行って発行された電子証明書の発行日から起算して五年を超えない日までに満了するものである」必要があります。従って、②となります

2. その他		
No.	相談内容	回答内容
1	認証局のホームページ内に一般財団法人日本情報経済社会推進協会（JIPDEC）のロゴ、および「電子署名・認証センター」のサイトにリンクすることに対して諸問題が生じないでしょうか？	認証局のホームページ内に一般財団法人日本情報経済社会推進協会（JIPDEC）のロゴの使用、および「電子署名・認証センター」のサイトへのリンクについてはまったく問題ありません。

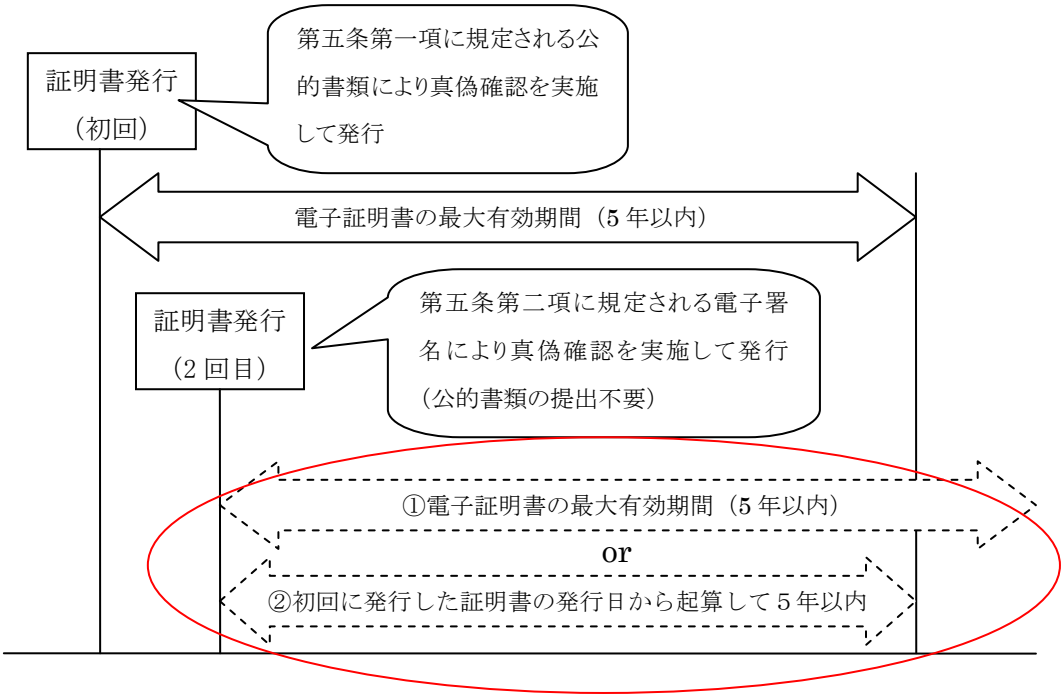

図 1.1　No.7 の参照図

2.1.2 2.2.2 認定認証事業者からの問い合わせ Q&A（認証業務の用に供する設備編）

この問い合わせ Q&A は、問い合わせ分類②の認証業務の用供する設備についてまとめたものです。

1. 認証設備関連

1.1 認証設備室

No.	相談内容	回答内容
1	認証設備室の設備要件としてどのような書類で確認されるのでしょうか？	①調査表項番1541 指針第七条第二号ハの要件が確認できる書類が必要となります。消防法第十七条第三項の規定に基づく定期点検について半年毎に実施されていることが、「消防用設備等点検結果報告書」により確認できること、及び「検査結果通知書」により消防用設備に対する消防署の検査が実施済であることが確認できるもの。 ②調査表項番1571、1581、1591 指針第七条第三号イ、ロ、ハの要件が確認できる確認通知書、検査済証等の書類が必要となります。 イ 建築されている土地の地盤が地震被害のおそれの少ないものであること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。（指針第七条第三号イ） ロ 地震に対する安全性に係る建築基準法（昭和二十五年法律第二百一号）又はこれに基づく命令若しくは条例の規定に適合する建築物であること。（指針第七条第三号ロ） ハ 建築基準法に規定する耐火建築物又は準耐火建築物であること。（指針第七条第三号ハ） 【関係法令】 指針第七条第二号ハ 指針第七条第三号イ 指針第七条第三号ロ 指針第七条第三号ハ
2	認証設備室のパーティション（ケージ）に対して、防音に関する要件がありますか？	指針第七条第二号ロの要件に関しましては、防音を要件として求めてはいません。 【関係法令】 指針第七条第二号ロ

		施行規則第六条第十五号へ
3	認証設備室の入室ドアの設置を変更（開閉を逆に）する場合は、変更認定の申請が必要でしょうか、またどのような対応が必要でしょうか？	電子署名法第四条第二項第二号の事項の変更には該当しないものと思われますので、変更認定の申請は必要ありません。 以下の事項に留意いただき、次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 ・ご説明資料に基づく実施内容、工事手順、工事期間中の入退室管理の遵守 ・上記遵守状況が確認できるチェックリスト付き工事手順書の作成及び記録 ・更新調査時に実施した発報テストと同様のテストの実施及び記録 ・以上を包括的に取りまとめた認証業務用設備及び施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録の作成 【関係法令】 電子署名法第四条第二項第二号
4	認証設備室と同じ区画に、新しく一般の認証設備室を増設する場合は、変更認定の申請が必要でしょうか？	認定認証業務の認証設備室と同一区画に新しく一般の認証設備室を増設することは、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】 電子署名法第四条第二項第二号
1.2. 入退出管理システム		
No.	相談内容	回答内容
1	入退出管理システムの更改はどのような手順で実施することが可能でしょうか？	電子署名法に基づく特定認証業務の認定に係る指針第四条第一号に係るイ及びハの措置に関する変更認定を受ける必要があります。 下記に手順の一例を示します。 ①指定調査機関への相談（資料の事前確認） ②変更認定の申請 ③現行の入退出管理システムに影響を与えない新設される生体認証装置の事前工事施工

		（下記④の切り替え工事を24 時間以内に完了させるため必要に応じて実施） ④生体認証装置の切り替えを実施する。切り替え工事は当該工事日中24 時間以内に終わることを想定している。また工事完了後は切り替え前と同様に、既設設備による映像監視を実施する。 ⑤④の工事の翌日、指定調査機関による実地調査を実施 ⑥調査内容の主務大臣への通知 ⑦主務大臣による変更認定 ⑤の実地調査については、④を実施した連続する翌営業日の調査が可能となるようにスケジュール調整いただく必要があります。 ④の工事実施中はIA 業務の運用要員（宣誓書を提出して要員資格を有する者）により立会いと共に目視にて警備･監視を実施するとともに、映像記録を残す(指針第四条第一号二の措置)ことにより、また⑤の実地調査以降は、IA 業務は通常どおり実施されることになるため、指針第四条第一号ハ及び二の措置により、認証設備の安全基準を担保して下さい。 【関係法令】 指針第四条第一号イ・ロ・ハ・ニ 指針第七条第二号ホ 指針第十三条第一号 施行規則第六条第十五号イ
2	入退出管理システムの管理用ハードウェアおよびその周辺機器を更改する場合は、変更認定の申請が必要でしょうか？	入退室管理システムの管理画面GUI を制御するためのハードウェア及びその周辺機器に関する部分のみをリプレースすることは、電子署名法第四条第二項第二号の事項の変更には該当しないものと思われますので、変更認定の申請は必要ないと思われます。 【関係法令】 施行規則第九条
1.3.　認証業務用設備 1.3.1　軽微な変更（施行規則第九条）		

No.	相談内容	回答内容
1	サーバ機器を更改する場合は、変更認定の申請が必要でしょうか？	サーバ等を既設の設備と同等以上の性能を有する設備へ変更することは、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 またその他のサーバにつきまして、利用者の個人情報や一部規程類が含まれている場合、従来と同様の漏えい、滅失又はき損の防止措置を担保いただくことにより、変更認定の申請は必要ありません。 【関係法令】 施行規則第九条
2	登録局内のハードウェア、ソフトウェアの更改および新規追加する場合は、変更認定の申請が必要でしょうか？	認証業務用設備に該当しない設備については、変更認定の申請は必要ありません。 認証業務用設備に該当する設備については、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 【関係法令】 施行規則第九条
1.3.2　ハードウェア更改（変更認定が必要な場合）		
No.	相談内容	回答内容
1	HSM（ハードウェアセキュリティモジュール）を後継機種に更改する場合で、運用手順に変更はない場合でも、変更認定の申請が必要でしょうか？	HSM の変更に伴い、電子署名法に基づく特定認証業務の認定に係る指針第十四条に係る措置（調査表では 3Exx 項番）に変更が生じる場合には、法第四条第二項第二号又は第三号の事項の変更に該当する可能性があります。 特にHSM の変更に伴い、サーバーとの接続形態が変更になる場合は、発行者署名符号の廃棄時における措置について、仕様上や運用時の変更等が発生しないか、HSM の仕様や手順書の記述内容に即してご検討・ご確認ください。 【関係法令】 法第四条第二項第二号 法第四条第二項第三号
1.3.3　ハードウェアの廃棄または機器増設		

No.	相談内容	回答内容
1	システム更改後のサーバ機器の撤去は、変更認定が必要でしょうか。また、指定調査機関に事前事後に連絡が必要でしょうか？	認証業務用設備に該当しない設備につきましては、変更認定の申請は必要ありません。 実施に際しましては、施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に指定調査機関による調査を受けていただきますようお願いいたします。 認証業務用設備に該当する設備についても○○であれば電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要がない場合があります。 【関係法令】 施行規則第四条 施行規則第九条
2	IA サーバのデータベースをRAID装置からIA サーバの内蔵ディスク（RAID）に変更する場合は、変更認定の申請が必要でしょうか？	IA サーバの内蔵ディスク（RAID）が、従来のRAID 装置と同等以上の性能を有する場合（RAID の規格を含む）には、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 【関係法令】 施行規則第九条
1.3.4　ソフトウェアのバージョンアップ及び設定変更		
No.	相談内容	回答内容
1	PKI システムのバージョンアップ（サポート切れおよびSHA256 対応の為）する場合は、変更認定の申請が必要でしょうか？	PKI システムのバージョンアップに関しては、現環境のPKI システムで使用している機能が新環境においても提供されることにより、業務に関する措置状況には変更が生じないとのことなので、PKI システムのバージョンアップを実施することは、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 【関係法令】 施行規則第九条
2	IA サーバ上で稼働しているCRLの生成及び更新プログラムを改修する場合は、変更認定の申請が必	CRL の生成及び更新プログラムの改修を実施されることは、電子署名法第四条第二項第二号及び第三号の事項の変更には該当せず、変更認定の申請は必要あり

	要でしょうか？	ません。 【関係法令】 法第四条第二項第二号 法第四条第二項第三号
3	RA 登録サーバとIA サーバ間の通信モジュールのバージョンアップおよび証明書発行失効システムのバージョンアップする場合は、変更認定の申請が必要でしょうか？	電子署名法施行規則第九条に定める軽微な変更に相当すると考えられ、変更認定の必要はないと思料します。 【関係法令】 施行規則第九条
1.3.5　認証設備室と登録用端末室（あるいはIC カード発行室）とのネットワーク接続		
No.	相談内容	回答内容
1	認証設備室内のIA サーバとファイアウォールで接続された登録用端末機の構成を、IAサーバと登録用端末機を直接ネットワーク接続する構成に変更することは、問題ないでしょうか？	電子署名法施行規則第九条に定める軽微な変更に該当するものと思料します。 【関係法令】 施行規則第九条
2	認証設備室に設置された登録局との接続用ルータを更改する場合は、変更認定の申請が必要でしょうか？	認証設備室に設置された登録局との接続用ルータをリプレースすることは、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 施行規則第十二条第一項第四号ホの認証業務用設備及び第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、設定変更後の更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第九条
3	認証設備室間（認証設備室とIC カード発行室）のネットワーク接続（モデム接続からイーサネット回線接続）を変更する場合は、変更認定の申請が必要でしょうか？	認証設備室が設置されている建物内における接続変更ということで、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】

		法第四条第二項第二号
1.3.6　その他		
No.	相談内容	回答内容
1	認証設備室内でラックを移動する場合は、変更認定の申請が必要でしょうか？	ラックの移動で認証業務用設備に変更がなければ、変更認定の申請は必要ありません。 【関係法令】
1.4　IDS（侵入検知システム）機器の更改		
No.	相談内容	回答内容
1	IDS、IDS センサおよびIDS 管理サーバを更改する場合やIDS ソフトウェアをバージョンアップする場合は、変更認定の申請が必要でしょうか？	IDS、IDS センサおよびIDS 管理サーバを更改する場合やIDS ソフトウェアのバージョンアップする場合は、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 【関係法令】 施行規則第九条
2	ファイアウォールおよび侵入検知システム機能を統合する場合は、変更認定の申請が必要でしょうか？	電子署名法に基づく特定認証業務の認定に係る指針第五条第一号に規定される不正なアクセス等を防御するためのファイアウォール及び不正なアクセス等を検知するシステムは、調査表の1213及び1214で別々に確認させていただいている通信機器であり、それぞれに調査結果を主務省に報告しております。それぞれの機能が統合され、1 台の通信機器にて署名法の2 つの要件を満たすことについては、変更認定を申請いただき、確認する必要があります。 【関係法令】 施行規則第四条第三号 指針第六条第一項第一号
1.5　遠隔監視装置及び映像記録装置 1.5.1　遠隔監視装置		
No.	相談内容	回答内容
1	監視センター内でフロアレイアウトを変更する場合は、変更認定の申請が必要でしょうか？	現状の設備、運用、体制（委託契約を含む）に一切変更がないことが添付資料にて確認できることにより、変更認定の申請は必要ありません。 変更に際しては、作業内容を記録した帳簿を作成した上で、次回更新調査時に、指定調査機関による調査を

		受けてください。 【関係法令】 施行規則第四条 指針第四条第一号ニ
2	漏水監視装置から通知を受ける先を変更する場合は、変更認定の申請が必要でしょうか？	漏水監視通知先を、現在の場所と同様に常時、監視者が駐在する場所に設置された同機能の設備に変更される場合には、変更認定の申請は必要ありません。 実施に際しましては、施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に指定調査機関による調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第四条
3	認証局内の外部セグメントから認証設備室内のサーバへPing 監視を行うように変更する場合は、変更認定の申請が必要でしょうか？	内部ファイアウォールに対するルール設定の変更が、Ping 監視に必要な最小限のポート設定に限定される限りにおいて、お問い合わせいただいた範囲内であれば、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】 施行規則第四条
1.5.2　映像記録装置		
No.	相談内容	回答内容
1	映像記録装置を更改する場合は、検討している更改の手順で問題ないでしょうか？ 映像記録データが欠損しない方法で更改する手順で実施する予定です。	映像記録装置リプレースに関して、お問い合わせいただいた添付資料の範囲内であれば、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の必要はないと思われます。 【関係法令】 指針第四条第一号ニ
2	映像記録端末を更改する場合は、変更認定の申請が必要でしょうか？ 交換にあたって、画像サイズ、記録時間間隔、記録する映像をカメ	上記お問合せいただいた範囲内で、映像記録装置を交換することは、電子署名法施行規則第九条に定める軽微な変更に相当し、変更認定の必要はないと思料いたします。 認証業務用設備及び規則第四条各号の基準に適合す

	ラ台数の変更はありません。ただし、今後の保守性を考慮し、PC 自体を交換するため、OS やハードディスク容量、映像閲覧プログラムが後継のものにバージョンアップされます。	るために必要な設備の維持管理に関する記録を作成いただき、実施後の更新調査時に、指定調査機関による調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第九条
3	認証設備室内の監視カメラを変更する場合は、変更認定の申請が必要でしょうか？	○○の範囲内において映像記録装置で使用している監視カメラを交換することは、電子署名法施行規則第九条に定める軽微な変更に相当し、変更認定の申請は必要ありません。 なお、監視カメラの交換作業実施に際しましては、以下の事項に留意いただき、下記留意事項の実施結果を含んだ施行規則第十二条第一項第四号ホの認証業務用設備及び第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、交換作業後の最初の更新調査時に、指定調査機関による調査を受けていただきますようお願いいたします。 ●交換作業中は、認証設備室及び共同RA 室内に入室権限者2 名以上からなる監視者を配置するなどにより、厳重な認証設備室への立ち入り禁止措置を実施すること。 ●映像記録（指針第四条第一号ニに基づく要件）の欠損期間について、必要最小限となるように配慮すること。 ●交換作業中は、IA 側要員による認証業務用設備の直接操作等、認証設備室及び共同RA 室における当該業務の運用に関わる作業を行わないこと。 ● 作業完了後に、入退室管理装置のログにより、映像記録が欠損する時間帯に認証設備室及び共同RA 室に対する不正な入室者がなかったことを確認すること。 【関係法令】 施行規則第九条 施行規則第十二条第一項第四号ホ
4	認証設備室内の監視カメラのモニ	遠隔監視用のモニタを、現在の事務室と同じセキュリ

	タを事務室〔認定取得済〕に移動する場合は、変更認定の申請が必要でしょうか？	ティレベルが保たれる別の事務室に変更される場合には、変更認定の必要はありません。 実施に際しましては、モニタ移設中の認証設備室への立ち入りを禁止いただいた上で、施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に指定調査機関による調査を受けて下さい。 【関係法令】 施行規則第四条
5	映像記録措置に障害が発生し、ディスク交換が必要となりましたが、原因究明のために旧ディスクを保守事業者に調査依頼することは、問題ないでしょうか？	ディスクに保存されている映像は、発行業務そのものが記録され、CPS に記された「当該情報を含む記憶媒体」に該当しないか確認が必要です。この場合特に、障害を起こした機器等の修理・保守等を依頼される際に、御社との間で守秘義務契約等を結ぶ必要があると考えます。 また、旧ディスクの廃棄にあたっては、完全消去を実施した後に物理破壊することが望ましい処置と考えます。処置を委託する場合には、廃棄等の実施記録に係る報告書を徴取し、保存することとしてください。 【関係法令】 施行規則第四条
6	映像記録装置に障害が発生し、監視が停止する期間が発生しましたが、どのような対応が必要でしょうか？	遠隔監視装置は、電子署名法に基づく特定認証業務の認定に係る指針第四条第一号ニに係る要件です。 本件に係る障害の記録及び障害に係る影響等の記録は次回の更新調査時に確認しますので、障害に関する記録帳簿、当該期間の入退室記録(認証設備室)、及び監視装置の修理記録等を保存いただきますようお願いいたします。 【関係法令】 指針第四条第一号ニ
2.　登録用端末室 2.1　登録用端末室		
No.	相談内容	回答内容
1	登録用端末室への入室管理をテン	電子署名法に基づく特定認証業務の認定に係る指針

	キーによる暗証番号入力からICカードによる認証に変更することは、問題ないでしょうか？	第四条第二号のとおり、登録用端末室は、「登録用端末設備又は利用者識別設備が設置された室であって、認証設備室に該当しないもの関係者以外が容易に登録用端末設備又は利用者識別設備に触れることができないようにするための施錠等の措置が講じられていること。」が要件となっております。入室管理をお問い合わせのように変更することは、特に問題はありません。 登録用端末室専用カードの発行及び管理について、認証業務規程及び事務取扱要領等に明確かつ適切に規定し、規定に則した入室管理を実施して下さい。 【関係法令】 指針第四条第二号
2	登録用端末室の縮小のために隔壁を移動する場合は、変更認定の申請が必要でしょう か？ ・「生体認証ドア」および「物理鍵ドア」の位置を変更 ・登録端末室の隔壁を室内に向けて移動。 ・調査表の項番115x、3C56 の項目に変更なし ・隔壁は現状と同様、床から天井までを仕切るものを使用 ・工事の際には、登録局管理者が立会い、管理者用として使用しているキャビネット を他の書庫と同一のものに変更	室の区画措置（隔壁の材質を含む）、扉の施錠措置（物理鍵の管理方法を含む）、登録用端末設備のLAN 構成、登録用端末設備から発行局側への遠隔地間接続方式、登録用端末設備室内の帳簿の保存状況措置等、認定を受けている登録用端末設備室及び登録用端末設備に関する現在の措置状況を変更せずに、登録端末用設備室の一部の区画を変更することは、電子署名法第四条第二項第二号及び第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 実施に際しましては、以下の事項にご留意いただき、変更後の更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。なお、登録端末室の区画変更について、そのすべてが軽微な変更に値するものではないので、同様の変更に関しましては、事前に必ず指定調査機関までお問い合わせをいただきますよう、併せてお願いいたします。 ●工事中における、施行規則第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止 ●工事中における、指針第四条第二号に定められている、関係者以外が容易に登録用端末設備に触れることができないようにする措置の実施と記録の作成 ●認証業務用設備及び施行規則第四条各号の基準に

		適合するために必要な設備の維持管理に関する記録の作成 また、管理者用キャビネットの変更に関しましても、キャビネットのみの変更で、帳簿書類の記載内容の漏えい、滅失又はき損の防止のための措置状況に変更がないならば、変更認定の申請は必要ありません。 【関係法令】 指針第四条第二号 施行規則第十二条
3	登録用端末室の一面をガラス面とする場合は、ガラス面に対応措置をすることで、登録用端末室としての要件を満たすでしょうか？ 登録用端末室のガラス全面に貼付する製品は、「警察庁及び関連省庁と建物部品関連の民間団体から成る「防犯性能の高い建物部品の開発・普及に関する官民合同会議」が 公表している「防犯性能の高い建物部品目録」に型番登載されている製品」です。	提示の防犯性能の保証等を考慮し、特殊な方法を用いなければ、容易に破壊できない状態になる場合には、指針第四条第二号に沿った処置と思料いたします。 【関係法令】 指針第四条第二号
2.2　登録用端末設備		
No.	相談内容	回答内容
1	発行局と接続する登録用端末を複数台にすることは、問題ないでしょうか？	発行局側との通信時には、指針第五条第二項に基づき設備の誤認等防止措置が必要です。登録用端末の複数使用は問題ないと考えますが、発行局側のファイアウォールの設定等により、発行局側認証業務用設備へ接続可能な登録用端末が限定されるように制限することが望ましいと考えます。 【関連法案】 指針第五条第二項
2	登録用端末設備を撤去する場合は、変更認定の申請が必要でしょうか？	更新認定調査において、撤去される設備について施行規則第四条第二号及び第三号で求められる認証業務用設備の動作に関する記録を確認しますので、それら

		の記録を保存すれば、変更認定の申請は必要ありません。 【関係法令】 施行規則第四条第二号
3	登録用端末室設備を、施錠可能なラック内に設置するように変更する場合は、変更認定の申請が必要でしょうか？	電子署名法に基づく特定認証業務の認定に係る指針第四条第二号に基づき関係者以外が容易に登録用端末設備に触れることができないようにするための措置について、小型のPCであるRA操作端末を移動が容易に行えないラックに施錠して格納することで、より安全性を向上させる措置であり、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】 施行規則第四条第二号
4	登録用端末室に社内ネットワークに接続する端末を設置することは、問題ないでしょうか？	登録用端末室に社内ネットワークに接続された端末の導入をしても問題はありません。なお、当該端末は登録用端末設備のセキュリティを落とすことなく使用されることが担保され、利用基準を定めて管理されることが望ましいと思料いたします。 【関係法令】 指針第四条第二号
5	登録用端末室内の機器の監視を実施することは、問題ないでしょうか？ ・登録用端末/管理サーバ(NW 機器を含む)からのSNMP Trap やサーバの生死, 性能(CPU使用率)等の異常監視を行う. ・社内業務担当者が異常監視を行う	社内業務担当者が異常監視を行うことは問題ないと考えますが、異常検知時にトラブル対応に当たるのは当該認証業務担当者である必要があります。 【関係法令】 指針第五条
3.　その他 3.1　リポジトリ		
No.	相談内容	回答内容
1	リポジトリソフトウェアのタイム	電子署名法第四条第二項第二号又は第三号の事項の

	アウト値を変更する場合は、変更認定の申請が必要でしょうか？	変更には該当せず、変更認定の申請は必要ありません。 【関係法令】 施行規則第六条十一号
2	リポジトリサーバのOS およびソフトウェアをバージョンアップし、全てのセキュリティパッチを適用する場合は、変更認定の申請が必要でしょうか？	リポジトリサーバのOS およびソフトウェアのバージョンアップ等を実施することは、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 【関連法案】 施行規則第九条
3	リポジトリサーバの改ざん検知ソフトウェアのバージョンアップする場合は、変更認定の申請が必要でしょうか？	電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。 【関係法令】 施行規則第九条
3.2　NTP（時間同期）		
No.	相談内容	回答内容
1	外部 NTP サーバと時刻同期する場合は、変更認定の申請が必要でしょうか？	各ファイアウォールに対するルール設定の追加が、時刻同期に必要な最小限のポート設定に限定される限りにおいて、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関連法案】 指針第五条
3.3　ログ収集		
No.	相談内容	回答内容
1	ログ収集用サーバの機能を不正侵入検知システム（IDS）に統合する場合は、変更認定の申請が必要でしょうか？ 〈添付資料＞ ログ収集用サーバの機能統合説明資料	機能を統合することで不正侵入等を検知するシステムの機能低下がないことが保障される限りにおいて、変更認定の申請は必要ありません。 また実施後、不正侵入等を検知するシステムの安定稼働が確認されるまでの期間は特に、定期的な機器の死活確認等を実施いただき、不正侵入等を検知するシステムが停止することのないように監視を強化いただきたいと思います。

		【関係法令】 施行規則第四条
2	ログ送信先である受付IP アドレスを変更する場合は、変更認定の申請が必要でしょうか？ 特定認証業務の各設備において以下設定を変更する必要が生じます。 ①「ログ監視サービス」の受付IP アドレス変更に伴う、認証設備室に存在するログ監視対象サーバのログ送信先の変更。 ②「ログ監視サービス」の受付IP アドレス変更に伴う、認証業務設備のLayer3 スイッチの経路制御ルールの変更（通信可能なIP アドレスを変更）。	ログ監視サービスの受付IP アドレス変更に伴う変更処理に関して、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 実施に際しましては、認証業務用設備及び施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、設備変更後の各特定認証業務更新調査時に、指定調査機関による実地調査を受けてください。 【関係法令】 施行規則第四条
3.4　認証業務用設備等の災害の被害を防止するために必要な措置		
No.	相談内容	回答内容
1	認証業務用設備を設置しているデータセンターでCVCF を更改する場合は、変更認定の申請が必要でしょうか？	電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 以下の事項に留意いただき、CVCF 更新実施後の更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 ① 映像記録装置、監視機器等の停止に伴う認証設備室への入退室管理制限、及び在室監視の実施 ② ①の実施状況が確認できる記録の作成 ③ 施行規則第四条第五号の基準に適合するために必要な設備の維持管理に関する記録の作成 ④ 緊急対応に係るバックアップ等の準備及び電源回復時の実施手順及びシステム動作状況確認リスト等の準備 ⑤ LDAP サーバ停止に伴う利用者、署名検証者、BCA 等への事前周知

		⑥ 停電予定時間を大幅に超過し、CRL の自動更新処理等に影響が及んだ際に利用者、署名検証者、BCA 等へ周知するための連絡方法、及び実施体制の整備 ⑦ 停電予定時間を大幅に超過し、CRL の自動更新処理等に実際に影響が及んだ際の、利用者、署名検証者、BCA 等への周知、連絡の実施状況の記録、及び指定調査機関への報告 【関係法令】 施行規則第四条
3.5　セキュリティ対策		
No.	相談内容	回答内容
1	セキュリティパッチの更新作業を実施する場合は、変更認定の申請が必要でしょうか？	電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の必要はありません。 認証業務用設備及び施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第九条
2	ファイアウォールの設定（ウィルス対策サーバの移設）を変更する場合は、変更認定の申請が必要でしょうか？	規定されたネットワークフィルタリングポリシーに従い、当該ファイアウォールの設定を変更することは、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】 指針第五条第一号
3.6　認証業務用設備以外の軽微な変更		
No.	相談内容	回答内容
1	認証業務用プリンターを更改する場合は、変更認定の申請が必要でしょうか？	認証業務用プリンター交換に伴う作業内容を実施することは、変更後のプリンターが機能・性能面において当該業務に必要な要件を満たしていれば、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の申請は必要ありません。

		【関連法案】 施行規則第九条
2	外部ファイアウォールの機種、構成変更、および外部ファイアウォールログ収集方法の変更を行う場合は、変更認定の申請が必要でしょうか？	外部ファイアウォールは、システム設計書にて設計されている外部ファイアウォールの設定値と同等のルールを新ファイアウォールに設定いただく場合には、変更認定の必要はありません。 実施に際しましては、施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に指定調査機関による調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第四条
3	WEB サーバ、LDAP サーバ、Syslog サーバを更改し、認証設備室外に設置する場合は、変更認定の申請が必要でしょうか？	外部ファイアウォールの設定値に関して、システム設計書に基づき現行と同等のルールが設定される限りにおいて、電子署名法施行規則第九条に定める軽微な変更に該当し、変更認定の必要はありません。 以下の事項に留意いただき、設備変更後の更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 ●施行規則第四条第三号の認証業務用設備の動作に関する記録の保存（【運用の変更箇所・理由】③に関連し、保存されている記録） ●認証業務用設備及び施行規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録の作成 【関係法令】 施行規則第九条
4	自動封入封緘機の更改する場合は、変更認定の申請が必要でしょうか？	利用者署名符号の活性化に使用するPIN の出力を行う場合は、盗聴、改変防止等の措置を講じている必要があります。お問合せのPIN 印刷の変更に伴いご提案される給料明細方式及び半自動封入封緘方式が、RA 発行業務発行担当の作業内でPIN の内容を見ることが容易には難しいものである場合には、変更は可能であると考えます。どちらの方式でも可能だと思われま

		すが、RA 発行業務発行担当者が見ることがより難しい方式が望ましいと考えます。 PIN 印刷の仕組みの変更は必ずしも業務運用上の変更とはならず、この場合変更認定の申請は必要ありません。 なお、実施にあたり関係する規程類の変更、変更する仕組みに係る仕様書の作成、関係者への教育訓練の実施及び変更した内容の記録を残すようにして頂ければと思います。 【関係法令】 規則第六条第三号
5	登録用端末設備室に録音機能付の電話機（利用者との電話連絡によるトラブル防止のため）を設置する場合は、変更認定の申請が必要でしょうか？	登録用端末設備室にヘルプデスク用録音機能付き電話機を設置することは、認証業務の認定に係る要件に該当しませんので、変更認定の申請は必要ありません。 【関係法令】
6	業務アプリケーションの不具合修正ならびに表示改善を実施する場合は、変更認定の申請が必要でしょうか？	業務アプリケーションのバージョンアップ及び仕様変更が、業務手順の変更に当たらない場合は、電子署名法第四条第二項第二号又は第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】 電子署名法第四条第二項第二号 電子署名法第四条第二項第三号
7	更新期限前に利用者宛てに更新通知メールを送る設定から、送信しない設定に変更する場合は、変更認定の申請が必要でしょうか？	電子署名法第四条第二項第二号又は第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 施行規則第十二条第四号ホの設備の維持管理に関する記録を作成いただき、次回の更新調査時に、指定調査機関による調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第九条

2.1.3 2.2.3 認定認証事業者からの問い合わせ Q&A（利用者の真偽確認編）

この問い合わせ Q&A は、問い合わせ分類③野利用者の真偽確認についてまとめたものです。

1. 利用者の真偽確認資料		
No.	相談内容	回答内容
1	「広域交付住民票」を真偽確認で求められる「住民票の写し」として扱ってよいでしょうか？	「広域交付住民票」は、住所地以外の市区町村窓口（住民基本台帳ネットワークに参加している市区町村の窓口）で、本人及び同一世帯の人が交付を受けられる「住民票の写し」です。ただし、本籍地、筆頭者の表示はされません。交付の請求は、住所地以外の市区町村で、住民基本台帳カードや運転免許証等で本人確認ができれば、例えば「住民票の写し等の請求書（広域交付用）」で同様に行うことができます。 以上のことより、「広域交付住民票」は、真偽確認で求められる「住民票の写し」として扱ってよいと思料いたします。 また、住民票記載事項証明書も、真偽確認で求められる「住民票の写し」に準ずるものとして扱ってよいと思料いたします。 実施に際しては、「住民票記載事項証明書」及び「広域交付住民票」を、「住民票の写し」と同様に取扱う旨を、利用者への説明書類、運用規程（CP/CPS）、事務取扱要領及び関連手順書等に規定し、利用者への周知を図るとともに関係者への教育・訓練を行い、記録を残して実施してください。 【関係法令】 施行規則第五条
2	本人死亡で失効する際の確認書類として「除籍謄本」を追加することは問題ないでしょうか？	戸籍に載っている方全員が、転籍や死亡などの理由で除籍になったときに発行されるのが除籍謄本であることから、本人死亡で失効する際の確認書類として「除籍謄本」を、運用規程（CP/CPS）、事務扱要領等に追記し、当該書類に基づき失効時の真偽確認を実施することは、特段の問題はないと思料いたします。
3	利用者が「日本に居住する日本国籍を持たない外国人」で、登録原票記載事項証明書に滞在期間が記載されていた場合は、滞在期間を超えた利用者の電子証明書を失効	滞在期間を超えた利用者の電子証明書は失効させる必要があるものと考えます。運用規程（CP/CPS）、利用者同意書の利用者の義務の項目に、滞在期間満了時に失効申請書を提出されない場合には、認証局事由で利用者の電子証明書を失効することを規定して

	さ せることが必要でしょうか？	おくことが必要と思われます。 ただし、利用申込み時において、滞在期間が記載された登録原票記載事項証明書を受理した場合は、少なくとも発行時において、滞在が許可された期間内であるかの確認が、必要と思われます。 【関係法令】 施行規則第五条
2. 真偽確認方法		
No.	相談内容	回答内容
1	公的個人認証サービスの電子証明書による電子署名で真偽確認を行う場合は、「住民票の写しまたは住民票記載事項証明書」と「印鑑登録証明書」の提出は不要とすることが可能でしょうか？	公的個人認証サービスにて発行された電子証明書による電子署名で真偽確認を行うことは、電子署名及び認証業務に関する法律施行規則の第五条第一項第二号において利用者の真偽の確認方法の一つとして定められており、業務の方法によっては適用可能と思います。この場合には、「住民票の写しまたは住民票記載事項証明書」と「印鑑登録証明書」の提出は不要となります。 公的個人認証サービスを利用した申請手続き等、全体的なシステム及び運用をどうするか等について、具体的イメージを検討してご提示ください。 【関係法令】 施行規則第五条第一項第二号
2	「住民票の写し」と「運転免許証」を対面により、真偽確認を実施することは可能でしょうか？	申込方法として、「住民票の写し」と「運転免許証」を対面により真偽確認を実施することを追加することは可能です。申込み方法や真偽確認手順の変更をともなうため、変更認定の申請が必要です。 【関係法令】 施行規則第一項第一号イ
3	氏名に関するふりがな（読み）が不明となった場合は、どのようにしたらよいでしょうか？	利用申込者から、あらためて、利用者のフリガナが確認できる公的資料（たとえば、パスポート等）を求めて、一致確認を進める必要があり、利用者からの申込みを安易に受け入れることは難しいと思料いたします。一致確認手順に他の資料を追加することは、真偽確認手順に変更がなければ、変更認定の申請は不要です。 事業者の責任で関係する規程類を改定し、利用者並びに関係者への周知を行い、記録を残して実施していた

		だくようお願いいたします。 【関係法令】 施行規則第五条
4	住所表記で【丁目】【番地】を【ハイフン】で省略することを許しておりますが、【ハイフン】をスペースにて省略することは可能でしょうか？	利用申込書の住所の記載は、原則として、住民票の記載どおりであることがもとめられます。住居表示制度に基づく、「丁目、番、号」と記載する住所表示の場合は、住居表示に関する法律に基づく「街区方式による住居表示の実施基準」（昭和39 年7 月30日自治省告示第１１７号、改正 昭和60 年7 月3 日自治省告示第１２５号）で、「丁目、番、号」をハイフンで省略しても住居表示が一致するとおもわれることから、ハイフンに省略することは容認されています。しかしながら、「丁目、番、号」をハイフンの変わりにスペースに置き換えることは同通達では容認されていません。「丁目、番、号」と「部屋番号」（建物名がない場合）および「建物名」と「部屋番号」の区別については、ハイフンをスペースにすることによりその区別が困難になることもあるため、利用申込書と住民票等の公的書類の記載内容が同一と見做すルーツを適切に規程し、業務を実施してください。 【関係法令】
5	住民票の写し及び申込書の住所表記で、番地とその枝番の間の「の」の有無の相違は同一とみなしてよいでしょうか？ 例） 例の１ （住民票）港区芝一丁目10番地11 →（申込書）港区芝一丁目10 番地の11 --- ○ 例の２ （住民票）港区芝一丁目10番地の11 →（申込書）港区芝一丁目 10 番地 11 --- ○	「○○番地△」と「○○番地の△」とが一致であるとの根拠が確認できない状況においては、原則、従来通りの解釈・運用で進めてください。 ただし、「例の1」の場合において、自治体が発行する「住民票の写し」の欄外に当該自治体が発行する「住民票の写し」においては、「の」を省略して記載する旨の断りがある場合は、「申込書」に「の」が記載されていても有効としても差し支えないと思料いたします。なお、この場合は、規程類でその取扱いについて、規定する必要があると思われます。 また、本判断を追加する場合の変更認定の申請は必要ありません。 【関係法令】

6	住民票の写しに「方書き」（建物名等）がない場合は、どのようにしたらよいでしょうか？	自治体により「方書き」が住民票の写しに記載されないところがありますので、以下のように対応してください。 ・住民票の写しに「方書き」が省略されている場合、利用申込書に「方書き」が記載されているものは「方書き」を除いて一致していれば、一致とみなす。 ・住民票の写しに「方書き」が記載されている場合、利用申込書に「方書き」が省略されているものは一致としない。 住民票の写し、利用申込書に「方書き」を省略したために、本人限定受取郵便が本人に届かない場合があります。郵便物の宛先には方書きを記載する等の対応が必要となることがあります。 【関係法令】

3. 漢字の置き換えについて

No.	相談内容	回答内容
1	「法務省 戸籍統一文字情報」を漢字置き換えの根拠とすることは可能でしょうか？	電子署名法上の真偽確認では、「住民票の写し」の記載内容と「利用申込書」の記載内容との一致を求めています。 「住民票の写し」に記載の文字が、ＪＩＳ第一水準もしくはＪＩＳ第二水準に存在する文字の場合は、「住民票の写し」に記載の文字をそのまま「利用申込書」に記載して頂く必要があります。 法務省ホームページ掲載の「法務省 戸籍統一文字情報」は「戸籍手続きオンラインシステム構築のための標準仕様書」の第2 章に記述されている選定基準（漢和辞典に掲載された正字等および俗字などの文字等）で選定されており、漢字置き換えの根拠とすることが可能です。 認証局として規程にその取り扱いを規定し、漢字置き換えを実施することが可能です。 【関係法令】

4. その他

No.	相談内容	回答内容
1	0S のフォントの相違により表示	利用申込書に記述される利用者名及び利用者住所等

	される文字が異なる場合は、どのようにしたらよいでしょうか？	は、本人確認の確認資料である「住民票の写し」等に記述される利用者名及び利用者住所等と同一である必要があります。利用者のPC 等の利用環境又は署名検証者のPC 等の利用環境が、認証業務のPC 等の利用環境と異なる場合、利用者又は署名検証者が視認する内容と、認証業務で視認する内容が異なる可能性があります。 本人確認を行うための真偽確認においては、認証業務内で確認する際に、「住民票の写し」等の文字が、利用申込書の文字と一致することが誤字俗字・正字一覧表又は通用字体に応じて整理した字体表（平成2 年10 月20 日法務省民二第5200 号通達別表2）等により確認出来る場合は、同一と判断されると思いますが、確認が出来ない場合は、不一致として取り扱うことになると考えます。 なお、環境の違いにより表示が異なることがある場合は、利用者及び署名検証者にリポジトリ等で周知して頂ければと思います。 【関係法令】
2	外国人の名前のファーストネームとミドルネームの間のスペースまたは「・（中点）」は同一のものとしてよいでしょうか？	外国人の名前をカタカナ表記で、ファーストネーム、ラストネーム、ミドルネームの区別のためにスペースまたは「・（中点）」は同一のものとして問題ないものと思います。 【関係法令】

2.1.4 2.2.4 認定認証事業者からの問い合わせ Q&A（認証業務の実施方法編）

この問い合わせ Q&A は、問い合わせ分類④の認証業務の実施方法についてまとめたものです。

1. 規程改定関連

1.1 認証事業者の社名等の変更に伴う規程の改訂

No.	相談内容	回答内容
1	社名あるいは認証業務を担当している部署･課名の変更に伴い、規程・申請書類関連・ホームページに係る問い合わせ先等を変更する場合は、変更認定の申請が必要でしょ うか？	社名あるいは認証業務を担当している部署･課名の変更に伴う規程･申請書類関連･ホームページの改訂は、業務の実施方法の変更には当たらないことから、電子署名法第四条第二項第二号又は第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 社名変更の場合は、公開情報のサイトでサイト証明書を使用している場合は、サイト証明書の変更についても対応するようにして下さい。 公開するホームページあるいは、リポジトリのURI 等について、変更が必要になった場合には、運用規程（CP/CPS）およびその他の規定類の修正を確認の上、実施するようにして下さい。 【関係法令】 施行規則第六条第十三号 指針第十二条第一項第一号
2	運用規程（CP/CPS）の連絡先から「代表者」欄を削除することは、問題ないでしょうか？	施行規則第六条第十三号及び指針第十二条第一項第一号では、 認証事業者の名称及び連絡先（住所、電話番号、ファクシミリ番号及びメールアドレス）としては、代表者名を記載することまでは規定していませんので、代表者欄を削除する変更を実施することは問題ありません。 【関係法令】 施行規則第六条第十三号 指針第十二条第一項第一号
3	更新調査時の指摘事項（提案事項）を実施する場合は、変更認定の申請が必要でしょうか？	更新調査時の指摘に、指摘事項（更新調査期間内で対応することが必要な事項）、提案事項（更新調査期間内に対応することが必要ない事項）とがあります。 更新時の提案事項について、規程類の誤記、記載漏れ保管物の追記、及び業務実態に即するための規程類の

		変更等、業務の変更にあたらない場合は、変更認定の申請は必要ありません。 【関係法令】 法第四条第二項第二号
4	業務方法が変わらないような規程や帳簿の書式変更を実施する場合は、変更認定の申請が必要でしょうか？	認証業務の手順、手続きの変更、設備、施設の変更、関係するソフトの変更は変更認定の申請が必要となる可能性がありますので、誤字の修正程度以外の修正はすべて変更認定の申請が必要かどうかお問い合わせ頂ければと考えます。 【関係法令】 法第四条第二項第二号
5	パスワード入力が必要ないと誤解する利用者が多いため、利用者宛に電子証明書と併せて送付する電子証明書の内容確認マニュアルを修正する場合は、変更認定の申請が必要でしょうか？	利用者宛に電子証明書と併せて送付する電子証明書の内容確認マニュアルの修正部分が問い合わせの範囲であれば、電子署名法の対象に該当せず、変更認定の申請は必要ありません。 実施に際しましては、貴認証局の判断の元、当該マニュアルの変更を実施してください。 【関係法令】
6	GPKI からの運用規程(CP/CPS)・事務取扱要領等の修正指示を実施することは、問題ないでしょうか？	GPKI からの修正指示により運用規程（CP/CPS）等の証明書プロファイルの定義を修正することは問題ありません。 相互認証証明書の有効期間の明確化と、誤字等の修正についてはお問合せいただかずに逐次実施して頂いても結構です。 【関係法令】

2. 帳簿の変更

2.1 利用申込書等の変更

No.	相談内容	回答内容
1	電子証明書の有効期間を新たに追加する場合に、現行の利用申込書に暫定的に有効期間を利用者に追記させることは、問題ないでしょうか？	利用申込書の本来の記述要件にない事項を利用申込者に要求することは、好ましい措置とは言えないと考えます。しかし、複数の有効期間が設定される利用申込書が印刷される仕組みがシステムに追加されるまでの短期において、暫定的に実施することを妨げるも

		のではないと考えます。 システムでプレプリントされる利用申込書に、利用申込者が有効期間を追記する場合、利用申込者が追記した部分については利用申込書の押印欄に押印された印鑑により修正印を押し、利用申込者が自分の意思で追記修正をしたことが分かるようにして下さい。 利用申込者には当該申込方式が暫定措置であること、及び申込手順が混乱しないように適切にリポジトリに公開して周知徹底を行うように実施して下さい。 なお、本件は、変更認定の申請は必要ありません。 暫定措置を実施するにあたり、事務取扱要領等の規程の一部に変更が生じるため、関係規程等に適切に規定し、実施して下さい。変更したことについての記録及び規程等は次回の更新調査時に確認させて頂きます。 また混乱を避けるためこの措置での対応期間を可能な限り短くするようお願い致します。 【関係法令】 施行規則第六条第四号
2	属性情報の確認資料を廃止し、利用申込書に確認情報欄を追加することは、問題ないでしょうか？	属性情報の確認資料を廃止し、利用申込書に確認情報欄を追加することで、利用申請に必要な資料を省力化する変更については、変更認定の申請は必要ありません。 利用申込書の改訂に伴い、運用規程（CP/CPS）、事務取扱要領等、関連規程類を変更する必要があり、また事前に利用者や業務担当者への十分な案内・周知も必要となります。 【関係法令】 施行規則第五条
3	失効申込書の注意書き（電子証明書の利用者本人が死亡した場合）、及び記載位置を変更する場合は、変更認定の申請が必要でしょうか？	失効申込書の改訂(注意書きおよび記載位置の変更)することは、変更認定の申請は必要ありません。帳票の変更に際しては、関連規程類の改訂、利用者への周知・徹底、関係者への教育・訓練につき、記録を残して、実施願います。 【関係法令】

		施行規則第六条第十号
4	利用者本人以外からの失効申請書に添付する書類を規程に追記する場合は、変更認定の申請が必要でしょうか？	利用者本人の死亡時においては、利用者以外からの失効申込が可能であることが運用規程（CP/CPS）に記載されていますが、組織等から失効申込を受け付ける場合は、どのような場合であるかが運用規程（CP/CPS）に明確に記載されていない場合には、本件の取扱いについて、利用者本人が所属していた組織であることを確認できる書類を含め運用規程（CP/CPS）に記載する必要があると考えます。 なお、所属組織からの失効申込手続きを追加し、失効申請方法及び受付後の真偽確認等の手続きを変更する場合は、変更認定の申請が必要と考えられます。 【関係法令】 施行規則第六条第十号 施行規則第十二条第二号
5	利用申請者に送付する発行通知書に有効期限を明記する場合は、変更認定の申請が必要でしょうか？	利用申請者に送付する発行通知書に有効期限を明記するように変更することは、電子署名法第四条第二項第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】
2.2　認証局内部の帳簿の変更		
No.	相談内容	回答内容
1	発行チェックシートなどの「日付」「判断者」欄の「記入」の規定を「署名もしくは押印」と改訂する場合は、変更認定の申請が必要でしょうか？	発行チェックシートなどの「日付」「判断者」欄を規定している事務取扱要領の記述を「記入」から「署名もしくは押印」と改訂することは、作業者、承認者の作業、承認日及び名前が分かる状態であれば特段支障がなく、変更認定の申請は必要ありません。 【関係法令】 施行規則第十二条第一項第一号ヘ
2	発行チェックリストの1 セットの枚数を削減する場合は、変更認定の申請が必要でしょうか？	「発行チェックリスト」の項目のレイアウトの変更が運用手順の変更を伴わない場合は、変更認定の申請は必要ありません。 変更内容については変更箇所が分かるように記録に残してください。

		【関係法令】 施行規則第十二条第一項第一号へ
3	管理簿の記入項目について、入力項目の重複等の冗長性の見直し及び記載誤りを二重線で訂正する変更を行う場合は、変更認定に申請が必要でしょうか？	帳簿の記載誤りがあった際に、訂正印が不要で二重線のみの訂正を可とすることは、業務の適切な記録の観点から妥当ではないと思料します。この他に関しましては、管理簿の見直しを実施されることは、電子署名法第四条第二項第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 【関係法令】
4	要員任命表に「所属欄」（外部委託している要員の明確化）を追加する場合は、変更認定の申請が必要でしょうか？	要員任命表に「所属欄」を追加することで、変更認定の申請は必要ありません。 実施に際しましては、次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 所属欄の記入に当たっては、委託先または派遣先の要員であることが判別できるようにしてください。 【関係法令】

3.電子証明書の格納媒体

3.1　IC カード

No.	相談内容	回答内容
1	電子証明書の格納媒体（IC カード）として別のメーカを追加する場合、あるいは格納媒体（IC カード）のバージョンアップを実施する場合は、変更認定の申請が必要でしょうか？	カードの仕様は電子署名法の認定基準に明確には定められていませんが、利用者署名符号が安全に格納可能な保存媒体であることが必要です。追加されるメーカのIC カードは、IC カードから端末間のデータ通信の転送プロトコルを定義する一部が異なる以外に、現行使用している製品の仕様と変更がなく、当該IC カードを使用することについて、変更認定の申請は必要ありません。 格納媒体(IC カード)のバージョンアップは同等程度の機能、性能を有するバージョンアップ設備であると考えられ、導入にあたって運用に係る手順に変更がないのであれば、電子署名法第四条第二項第二号又は第三号の事項の変更には該当せず、変更認定の申請は必要ありません。

		【関係法令】 電子署名法第四条第二項第二号 電子署名法第四条第二項第三号
2	IC カード不良時における再発行は、新たな真偽確認なしで発行することで問題ないでしょうか？	１回の利用申込みの意思により電子証明書を発行できるのは、原則として１回（複数枚の同時発行は可能）に限られるものと考えます。但し、いわゆる「初期不良」（電子証明書の使用開始直後に動作不良が発生した場合を含む。）の場合は、適切に利用可能な電子証明書が発行されていないと考えられることから、当該電子証明書を失効させた上で、電子証明書を（新たな真偽確認なしで）発行することが可能であると解されています。その場合の「初期不良」の判断基準については、認証事業者においてあらかじめ規定することが求められており、「初期不良」と判断し得る期間については、必要以上に長期にわたらないように留意する必要があります。 IC カードの記憶媒体としての初期動作不良については、IC カード不良として、表現を変更することは可能であると考えますが、当初より適切に利用可能な電子証明書を提供していなかったことについて、事務取要領等の内部規程において、従来の規定に変え、何らかのIC カード不良の判定基準を明確にして頂ければと考えます。 なお、認証局要員等が現地に出向いて、初期不良であることを確認することは必須ではないと考えますが、他の手段によって、認証局の責任に帰すものであることが確認出来る方法、例えば、利用者からの提示情報により、認証局の責任に帰すものであることが確認出来る場合は、利用者の実印が押印された書類等により、利用者の申し出の内容について担保することが必要であると考えます。 【関係法令】 施行規則第六条第三号
3	IC カード動作不良等の原因究明のために、検査を第三者機関に依	利用者署名符号を使用不可にするため、関係する電子証明書を失効した後、そのICカードの動作不良等の原

	頼することは可能でしょうか？	因究明のために、IC カードメーカやIC カードを検査する機関に調査を依頼することは可能であると考えます。 但し、電子証明書に記載されている個人情報が当該認証業務以外の第三者に公開される、又はその恐れがあることについて、予め利用者の同意が必要であり、調査委託契約等において、検査機関に対し、利用者署名符号（秘密鍵）の使用及び利用者署名符号の探査の実行等、利用者及び認証業務のセキュリティを脅かすような行為を行わないことを義務づける必要もあると考えます。 また、調査結果についても、外部への漏洩を防止する措置を講じる必要があると考えます。 【関係法令】 施行規則第六条第十五号ヘ

3.2　USB メモリ／CD-R

No.	相談内容	回答内容
1	電子証明書の格納媒体をFD から USB メモリまたCD-R に変更する場合は、変更認定の申請が必要でしょうか？	利用者署名符号の取扱に係る要件は、施行規則第六条第三号及び第三号の二であり、電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針第4 2.「認定認証事業者による利用者署名符号及び利用者署名識別符号の生成等」により、利用者署名符号の生成、転送、その出力（格納媒体への書き込み）、送付方法等に係る業務の実施方法の変更を伴う場合については、変更認定の申請が必要です。 【関係法令】 施行規則第六条第三号、第三号の二
2	電子証明書の格納媒体（USB メモリ）を、容量や型が異なるものに変更する場合は、変更認定の申請は必要でしょうか？	同等程度の機能・性能を有するバージョンアップと考えられるのであれば、電子署名法第四条第二項第二号又は第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 実施に際しましては当該変更に係る作業記録を作成し、関連する手順書等の修正を適切に実施し、次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。

		なお、USB メモリの選択にあたっては、価格等のほか、信頼性も考慮の上、利用者へ提供時にトラブルが発生するおそれの少ない製品を検討していただきますようお願いいたします。 【関係法令】 施行規則第六条第三号
3	電子証明書の格納媒体（CD-R）の券面に直接印刷するように変更する場合は、変更認定の申請が必要でしょうか？	電子証明書の格納媒体についての変更の場合、安全、確実に利用者に渡す要件により、その媒体の安全性を確認するため、変更認定の申請が必要となる場合があります。 しかし、今回のお問合わせの内容は、利用者署名符号の格納媒体の表面への必要情報の記載方法を、必要情報が記載されたラベルを貼付する方法から、直接、必要情報を利用者署名符号の格納媒体であるCD-R の表面に記載する方法に変更するというものであり、この変更による利用者署名符号の安全性への影響はないと思われることから、直接、CD-R の表面に記載する方法に変更することは可能であり、変更認定の申請は必要ありません。 実施にあたり、規程及び仕様書等において、必要情報の記載に関する一部の操作手順の変更等について、修正し実施して頂ければと考えます。 変更の実施にあたっては、認証事業者の責任のもと、関係する規程類の変更と関係者への周知、並びに、本業務の実施担当者に対する手順に関する教育・訓練をおこなうとともに変更の記録を残し実施してください。変更内容、運用状況等については、次回更新時に指定調査機関が確認いたします。 【関係法令】 施行規則第六条第三号
3.3	PKCS#12	
No.	相談内容	回答内容
1	電子証明書をPKCS#12 形式で「電子証明書格納媒体」に格納し、利用者に配布する場合の注意事項等	電子証明書（利用者秘密鍵含む）の発行形態として、PKCS#12 形式で電子証明書格納媒体に格納して利用者に配布することは電子署名法制度において問題あ

	があれば教えて下さい。 想定案としては下記を検討しています。 案１）認証局システムのメモリ上で利用者秘密鍵を生成し、直接「電子証明書格納媒体」内にPKCS#12 形式で格納する。利用者秘密鍵については、電子証明書格納媒体に格納後、認証局システム（メモリ上）から完全に消去する。 案２）認証局システムのメモリ上で利用者秘密鍵を生成し、一旦外付けHDD にPKCS#12 形式で発行する。利用者秘密鍵については、外付けHDD に発行後、認証局システム（メモリ上）から完全に消去する。 PKCS#12 は、証明書格納ソフトを利用して「電子証明書格納媒体」に格納する。電子証明書格納媒体に格納後は、証明書格納ソフトの完全削除機能を利用し、外付けHDD から完全に消去する。	りません。 想定案に対する主な注意事項は、次のとおりです。 ・外付けHDD にPKCS#12 を保存する場合は、PKCS#12 にアクセス権限を付加し、仮に外付けHDD を他のマシンに接続した場合でも、通常の操でPKCS#12 を読み取れないようにすること ・外付けHDD にPKCS#12 を保存する場合に、PKCS#12 を外付けHDD に保存してから、USB メモリに格納後、外付けHDD から完全に消去するまでに日を跨ぐようなことがある際には、外付けHDD の保管と管理に十分配慮すること。 利用者秘密鍵、PKCS#12 形式及びPIN 情報をメモリ上でハンドリングし、電子証明書格納媒体に格納後は、メモリ上から完全消去するとのことなので、特に問題はありません。 以上、注意事項に関しては、一般的な事項としてあげたものであり、必ずしも全てを網羅している訳ではありません。いずれにせよ、発行形態が追加になるのであれば、変更認定が必要になることから、発行形態が具体化し、詳細な発行方式や、それに伴う業務手順と規程類等の変更箇所が明確になった時点で、再度お問合せください。 【関係法令】 施行規則第六条第三号
2	電子証明書の格納媒体にPKCS#12 のPIN 情報（テキスト）を一緒に格納することは、問題ないでしょうか？	電子証明書格納媒体内に、PKCS#12 形式と共に、PKCS#12 のPIN 情報（テキスト）を一緒に格納して利用者に配布している認定認証事業者も存在します。 想定案に対する主な注意事項は、次のとおりです。 ・ 電子証明書格納媒体の利用者への配布は、本人限定受取郵便（基本型）を用いること ・ 可能であれば、PIN 情報は同一の電子証明書格納媒体には格納せず、別の媒体にすることがセキュリティ上望ましい。 ・ PIN 情報をDB 及び外付けHDD に保存する場合は、暗号化して保存すること ・ PIN 情報をDB に保存する場合は、DB のトランザク

		ションログにPIN 情報が残らないようにすること ・ 外付けHDD にPKCS#12 を保存する場合に、PKCS#12 を外付けHDD に保存してから、USB メモリに格納後、外付けHDD から完全に消去するまでに日を跨ぐようなことがある際には、外付けHDD の保管と管理に十分配慮すること。 以上、注意事項に関しては、一般的な事項としてあげたものであり、必ずしも全てを網羅している訳ではありません。いずれにせよ、発行形態が追加になるのであれば、変更認定が必要になることから、発行形態が具体化し、詳細な発行方式や、それに伴う業務手順と規程類等の変更箇所が明確になった時点で、再度お問合せください。 【関係法令】 施行規則第六条第三号
3.4　複数枚発行の電子証明書		
No.	相談内容	回答内容
1	1 枚の申込書で複数枚の電子証明書を発行している場合で、1 枚の電子媒体への複数枚の電子証明書の格納することは、問題ないでしょうか？	利用者署名符号の送付等につきましては、電子署名法施行規則第六条第三号の二にある「安全かつ確実に利用者に渡す」ことが要件です。同一の利用者に利用者署名符号を送付する場合、使用する記録媒体への記録数を変更することは、可能であると考えます。 利用者署名符号の送付方法を変更する場合、また送付時に利用者署名符号を記録する記録媒体を変更する場合、変更認定の申請が必要となる場合があります。しかし、本件は、それらには変更はなく、同一の利用者に利用者署名符号を送付する記録媒体への記録数を変更することであり、安全かつ確実に利用者に渡す方法に影響するものではないと思われることから、本件は変更認定の申請は必要ありません。 なお、実施にあたり、該当する規程を確実に改訂して実施して頂ければと考えます。 変更した規程等については次回の更新調査時に確認致します。

		【関係法令】 施行規則第六条第三号の二
4. 委託契約関連 4.1 外部委託範囲		
No.	相談内容	回答内容
1	認証局で担当する業務の全てを委託することは可能でしょうか？	法第四条の主旨は特定認証業務を行おうとする者を主務大臣が認定するものであり、施行規則第六条第十五号ハに照らし、業務の全てを委託することは適当ではありません。 【関係法令】 施行規則第六条第十五号ハ
2	登録業務の全てを外部委託する場合は、電子署名法上問題ないでしょうか？	施行規則第六条第十五号ハの規定により、認定認証業務の一部を他に委託することは可能であるが、登録業務の全てを外部委託することは不適合です。認証業務の定義（法第二条第二項）から、利用者の真偽確認の結果を元に電子証明書の発行の可否判断を最終的に行うことが必要です。 【関係法令】 施行規則第六条第十五号ハ
4.2 委託先(再委託)の変更 4.2.1 業務委託		
No.	相談内容	回答内容
1	認証局における作業の一部を外部委託、再委託する場合は、変更認定の申請が必要でしょうか？	認証局における作業の一部を外部委託、再委託することは、施行規則第六条第十五号ハの業務委託の変更にあたり、変更認定の申請が必要となります。 変更調査時には、当該契約書の内容（委託元の指示の遵守及び責任分担、保証等）を確認しますので、調査の対象となる契約書を準備してください。また、施行規則第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置の観点から、双方の契約書の保存場所・保管状況についても確認します。この他、事前に委託元から再委託先の変更に対する承認を得ておくことも必要となりますのでご注意願います。

		【関係法令】 施行規則第六条第十五号ハ 施行規則第十二条第一項各号
4.2.2　委託契約の変更		
No.	相談内容	回答内容
1	再委託先が商号変更する場合、再委託先と委託先間の基本契約書は、現状のままで問題ないでしょうか？	再委託先が商号を変更することに関して、変更内容としては商号の変更のみであり、業務の実施内容、実施場所、実施体制、管理体制等全く変更がないのであれば、変更認定の申請は必要ありません。 なお、商号変更があったことが分かるように何らかの文書等を契約書と合わせて保存いただきますようお願いいたします。 【関係法令】 施行規則第六条第十五号ハ
2	委託契約を管理している部門をアウトソーシングする場合は、変更認定の申請が必要でしょうか？	アウトソーシングに伴い保管場所や設備の変更、或いは契約名義人変更や再委託関係の変更がない場合には、再委託業務に係る委託契約の管理等の共通業務処理を子会社にアウトソーシングすることは、電子署名法施行規則第六条第十五号ハに係る業務の委託にはあたらないものと思われます。したがって、変更認定の申請は必要ありません。 【関係法令】 施行規則第六条第十五号ハ
3	業務委託先の会社の組織変更により会社分割が発生し、実際に業務を委託している会社と業務委託先との間に委託契約が結ばれる場合は、変更認定の申請が必要でしょうか？	新規に委託契約する場合に該当し、変更認定の申請が必要となります。会社分割先と契約される契約書、委託業務内容および帳簿保管措置について変更調査することになります。 【関係法令】 施行規則第六条第十五号ハ
4	委託先と再委託先との間の基本契約書の内容が修正される場合は、こ変更認定の申請が必要でしょうか？	委託先との契約書「基本契約書」の変更内容は、業務委託先の責任範囲や義務などの基本事項に変更がないものならば、変更認定の申請は必要ありません。 なお、契約書の保管に関しては、旧契約書及び新契約書は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10 年間の保存義務が課せられておりますので、認定を受けた保管キャビネットに保管いただき、次回の更新調査時に指定調査機関にて提示頂いた内容で契約がなされていることの確認が必要です。 【関係法令】 施行規則第六条第十五号ハ
4.2.3　派遣契約		
No.	相談内容	回答内容
1	認証業務の一部の委託を解除し、認証局の要員である職員または派遣社員が直接実施する場合は、変更認定の申請が必要でしょうか？	業務の実施場所、環境、人員管理方法等に変更が無ければ、電子署名法第四条第二項第二号又は第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 実施に際しましては、業務の実施場所、環境、人員管理方法等に変更が無いことを確認するために、以下の3 点につきまして、変更実施前に指定調査機関による確認を受けてください。 ・ 関連する規程、手順書等の改訂（案） ・委託先の帳簿書類の移動手順書（案） ・委託解除の記録(案) 【関係法令】 施行規則第六条第十五号ハ
4. 2. 4　業務委託管理		
No.	相談内容	回答内容
1	各担当毎にページが分かれている委託業務の報告書に担当者および管理者がそれぞれのページに押印することになっており、それを連続して記入することで管理者の押印を減らすように変更する場合、変更認定の申請が必要でしょうか？	月次報告書フォーマット変更および月次報告書資料作成に関して、内容に遺漏がないものとしていただくことで、お問い合わせいただいた内容の範囲内であれば、変更認定の申請は必要ありません。 【関係法令】 施行規則第六条第十五号ハ
5.個人情報の取り扱い		
No.	相談内容	回答内容
1	プライバシーマーク取得時の次の指摘事項への対応を実施すること	現在の申し込み時の流れのはじめに「個人情報の取扱いについて」のページを挿入し、個人情報の取扱の条

	は、電子署名法上、問題ないでしょうか？ ・重要事項説明の前に個人情報の取扱いについての確認画面（「個人情報の取扱いについて」）を追加し、利用者の同意を得る ・個人情報の収集時に、利用者への説明として不足する項目（個人情報保護管理者の氏名又は職名、所属及び連絡先等）を追加する	件に同意をいただいた方のみが、現在の申し込みの流れに到達できるようにしてプライバシーマークの要求を満たし、これまでの申し込みの流れについては変更しないご提案の方法は、特段の問題はないものと思料します。 ただし、このページの追加により、重要事項説明への同意をとばして直接申込書がダウンロードできるようにならないことを確認してください。 個人情報の収集時の利用者への説明として、不足する項目（個人情報保護管理者の氏名又は職名、所属及び連絡先等）を追加するために、運用規程（CP/CPS）および利用者同意書等に追加記述することは問題ありません。 【関係法令】 施行規則第六条第一号 施行規則第六条第十五号ヘ
2	利用者への重要事項説明に当たる利用者同意書に、個人情報の取り扱いについて詳細に記述し、郵送や手渡しの時の一緒に渡すこと、あるいは利用申込書のダウンロード 時に同時に利用者同意書が同一ファイルでダウンロードされること、かつ、利用申込書を作成支援するWeb 上のシステム利用時の同意画面で利用者同意書を表示することは、問題ないでしょうか？	個人情報を直接本人から収集する場合の措置として、運用規程（CP/CPS）への詳細記述を取りやめ、利用者に確実にわたる「利用者同意書」で対応することについては、特段問題はないと考えます。 【関係法令】 施行規則第六条第一号 施行規則第六条第十五号ヘ
3	個人情報を含む電子媒体を移送する場合、電子媒体を暗号化等でセキュリティ向上をはかることは、問題ないでしょうか？	個人情報の取扱いで、電子媒体に格納されたファイルを暗号化する手順を規程に追加することは特段の問題はないと考えます。 【関係法令】 施行規則第六条第一号 施行規則第六条第十五号ヘ
4	電子証明書の取得促進策として、	認証業務において得た情報を認証局以外の他部門に

	認証局以外の他部門に対して電子証明書取得者の情報を提供することは問題ないでしょうか？	情報提供することは施行規則第六条十五条への「利用者の真偽の確認に際して知り得た情報の目的外使用の禁止」に該当する恐れがあると思料します。 また、現在の運用規程（CP/CPS）や利用規程に記載してある個人情報の取扱の記述によっては、利用者が認証局の他部門に電子証明書の取得有無の情報を提供することに対して、利用者の同意を得ているとは判断できないと思われます。 【関係法令】 施行規則第六条第一号 施行規則第六条第十五号へ
5	認証局が債権者となった場合、債権者であることを証明するために利用申込書の写しを裁判所に提示することは問題ないでしょうか？	個人情報の取扱いについては、「利用者の真偽の確認に際して知り得た情報の目的外使用禁止」（施行規則第六条第十五項へ）に対応した規程を作成しており、司法からの要求に応じて個人情報を提供することを明確に述べていませんが、司法からの要求に応じて個人情報を提供することは、その規程の範囲であるものと思料します。 また、運用規程（CP/CPS）において、「調停、訴訟、その他の法的、裁判上または行政手続の過程において、機密保持対象である情報を開示することができるものとする。」と規定されるとともに、「利用規約」（個人情報の取り扱い）において「３．法的根拠に基づいて情報を開示するように請求があった場合、本認証局は法の定めに従い、法執行機関へ情報を開示することがあります。」としていることから、裁判所から申込みの事実に係る証明を求められた場合、法執行機関への情報開示として利用申込書の写し等を開示することは、可能であると思料します。 なお、開示を実施された場合は、その記録を規定に沿って作成し、保存してください。 【関係法令】 施行規則第六条第一号 施行規則第六条第十五号へ
6.利用者へのサービス変更		

6.1　サービス停止		
No.	相談内容	回答内容
1	有効期間〇年の電子証明書サービスを終了する場合は、変更認定の申請が必要でしょうか？	電子署名法第四条第二項第二号及び第三号の事項の変更には該当せず、変更認定の申請は必要ありません。 実施に際しましては、認証業務用設備及び規則第四条第各号の基準に適合するために必要な設備の維持管理に関する記録を作成していただき、以下の手順で進めていただきますようお願い致します。 まず、利用者に対して、ホームページ上で（必要に応じて、書面でも）「有効期間 〇年の電子証明書発行サービスの終了」の案内を行ってください。同時に利用者への公開資料（運用規程（CP/CPS）や利用申込書兼同意書等）に、サービスを終了する旨を追記して公開してください。案内を行う時期としては、署名法上、特に規定されていませんが、サービスの終了日まで、利用者への十分な周知期間（例えば、認証局廃止の場合の60 日前までなどを参考に）を取ってください。 サービス終了に伴う規程類(運用規程（CP/CPS）、事務取扱要領、業務手順書等）、各種帳票類(利用申込書兼同意書、利用申込書類チェックシート等）などの書類の改訂を行い、サービス終了日の翌日にホームページへの公開、業務の切り替えを行ってください。 運用規程（CP/CPS）の改訂に当たっては、有効期間 〇年の電子証明書が発行されていたこと(どのようなプロファイルのものが、いつまで発行されていたか）、発行済みの有効期間〇年の電子証明書は発行サービス終了後も引き続き有効であることについて記載しておいてください。 なお、本運用の変更にあたっては、業務関係者への教育・訓練を実施し、当該記録を残してください。 次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第六条第四号

6.2　有効期間		
No.	相談内容	回答内容
1	電子証明書の有効期間(2 年から1年)を変更する場合は、変更認定の申請が必要でしょうか？	現行の電子証明書の利用申込の受付手続き、真偽確認の審査手続き、電子証明書の発行手続きに基本的には手順の変更がないと思われることから、電子署名法第四条第二項第二号及び第三号の事項の変更には該当せず、変更認定の必要はないと思料します。 実施に際しましては、認証業務用設備及び規則第四条第各号の基準に適合するために必要な設備の維持管理に関する記録を作成していただき、以下の手順で進めていただきますようお願い致します。 まず、利用者に対して、ホームページ上で（必要に応じて、書面でも）「有効期間 2 年の電子証明書発行サービスの有効期間の変更」の案内を行ってください。同時に利用者への公開資料（運用規程（CP/CPS）等）に、当該サービスの有効期間を変更する旨を追記して公開してください。案内を行う時期としては、署名法上、特に規定されていませんが、両サービスの終了日まで、利用者への十分な周知期間（例えば、認証局廃止の場合の60日前までなどを参考に）を取ってください。 当該サービス終了に伴う規程類(運用規程（CP/CPS）、事務取扱要領等)、各種帳票類等の書類の改訂を行い、当該サービス終了日の翌日にホームページへの公開、業務の切り替えを行ってください。 運用規程（CP/CPS）の改訂に当たっては、有効期間 2 年の電子証明書が発行されていたこと(どのようなプロファイルのものが、いつまで発行されていたか）、発行済みの有効期間 2 年の電子証明書は発行サービス終了後も引き続き有効であること等について記載しておいてください。 なお、本運用の変更にあたっては、業務関係者への教育・訓練を実施し、当該記録を残してください。 次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 【関係法令】

		施行規則第六条第四号
2	有効期間 5 年の電子証明書を追加する場合は、変更認定の申請が必要でしょうか？	利用者に発行する電子証明書の有効期間は発行の可否判断日から起算して5 年未満であることが必要です。お問合わせのとおり有効期間が5 年の電子証明書を発行することは可能ですが、登録局で行われる真偽の確認及び発行承認の時期と、発行局で行われる電子証明書の発行処理が行われる時期が異なるため、電子証明書の有効期間(validity)の開始時刻(notBefore)が、真偽の確認及び発行承認時から一定期間空いた状態で開始されることを考慮に入れた有効期間の設定と、運用方法をご検討頂ければと考えます。 なお、登録業務システム等の変更に伴い、操作手順の一部に変更が生じることについても、利用者署名符号及び電子証明書の発行作業の主な運用方法に変更が生じない場合は、変更認定の必要はないと考えますが、確認のために、システムの変更内容、操作性も含む運用上の変更内容と手順書を含む規程類の変更内容について、ご提示頂ければと考えます。また運用規程（CP/CPS）には利用者に発行する電子証明書の有効期間は発行の可否判断日から起算して5 年未満であることを明確に規定して頂ければと考えます。 【関係法令】 施行規則第六条第四号
6.3　利用申込書		
No.	相談内容	回答内容
1	入力および印刷ができる利用申込書（EXCEL 形式）を利用者に提供する場合は、変更認定の申請が必要でしょうか?	申込者が電子証明書の利用を申し込むにあたりパソコンにダウンロードした利用申込書に利用者が入力および印刷ができるEXCEL 形式の利用申込書を提供することや、同様な方式による、電子証明書失効申込書（利用者用、所属組織用）、利用者情報開示申込書及び利用者情報変更届出書の作成ツールを提供する方法を追加し、利用者の申請に係る利便を図る変更について、各種申込書類の送付や受理後の真偽確認等の手続きに変更がない場合には、変更認定の申請は必要ありません。 実施に際しては、住民票の写し、登録原票記載事項証

		明書並びに登記事項証明書等にJIS 第一・第二水準以外の文字が記載されていた場合の利用申込者や申請者への説明方法を確定し、事務取扱要領等関連規程に規定するとともに利用者並びに関係者への周知と教育を行い、実施していただくようお願いいたします。具体的な、規程類等の修正内容については、指定調査機関が次回の更新調査時に確認しますので変更履歴が分かる形で保存しておいて頂ければと考えます。 【関係法令】
2	利用申込書を透かし印刷して利用者に提供することは、問題ないでしょうか?	利用申込者が記入する申請情報が不鮮明になる、又は他の文字と誤認される恐れがある等、利用申込者からの申請情報が正確に受付られない場合は、そのような発行申込書を使用することは適切ではないと考えますが、真偽確認の審査時に、支障なく利用申込者からの申請情報を確認することが出来るのであれば、そのような利用申込書を採用することは可能であると考えます。 【関係法令】
3	利用申込書の有効期限を利用申込書作成日から6 ヶ月以内とするように運用規程（CP/CPS）、事務取扱要領等を変更する場合は、変更認定の申請が必要でしょうか？	「利用申込書の有効期限を利用申込書作成日から6ヶ月以内とする」ことについては、提出された規程の範囲内では、貴認証局で事前に調整し、利用申込者に送付されている利用申込書の提出に関わる内容であり、電子署名法の対象外であることから、変更認定の申請は必要ありません。 【関係法令】
6.4　電子証明書の発行対象者		
No.	相談内容	回答内容
1	電子証明書の発行対象者として海外に居住（在留）されている方を追加することは、問題ないでしょうか?	電子証明書の発行対象者に日本国籍を有し且つ日本国内に居住される個人の方に加えて、海外に居住（在留）されている方を加えることは、電子署名法上は、利用者の真偽確認を規定している、施行規則第五条一項のただし書きにおいて、触れている代理人の委任状に関して、利用申込者本人が国外に居住する場合においては、これに準ずるものとの記述があるとおり、対

		象者について、特段の制限を加えていないと解釈できます。 具体的には、住民票の写しや印鑑登録証明書に準ずるものを利用して、真偽確認を実施する必要があると思料いたします。その他、実施に際しては懸念されている、「信書の問題、印鑑証明書の問題、証明書・PIN の受渡の問題、印鑑(サイン)の照合の問題等」について詳細に検討する必要があります。 また、変更認定にあたるか否かの判断を行うには、上記の対応等を踏まえた変更内容を具体的に提示していただく必要があります。 【関係法令】 施行規則第五条
2	電子証明書の発行対象者として外国籍を有する方を追加することは、問題ないでしょうか?	電子証明書の発行対象者に ①外国籍を有し、日本国内に居住(在留)されている方 ②外国籍を有し、海外に居住されている方 を加えることは、電子署名法上可能です。 ①「外国籍を有し、日本国内に居住(在留)されている方」の場合 外国人登録法第四条の三に規定する登録原票記載事項証明書を有する方については、利用申込者の実在性が確認できるため、電子証明書の発行対象者とすることが可能です。 利用申込者の実在性の確認に加えて、意思の確認をどのような方法（例：印鑑登録証明書若しくは、施行規則第五条第一項第一号ハの方法を用いて、利用者の意思を確認する）を用いるかや、利用申込書の作成並びに電子証明書の記載における、登録原票記載事項証明書に通称名が記載されている場合の扱い等を配慮する必要があります。 ②「外国籍を有し、海外に居住されている方」の場合 電子署名法施行規則第5 条で利用申込者の真偽の確認が可能な場合は、認定認証業務が発行する電子証明書の利用を行うことは可能であると考えます。 利用申込者の真偽確認に加えて、利用申込方法、証明書記載内容、証明書・PINの受渡方法等について詳細に検討する必要があります。

		【関係法令】 施行規則第五条
6.5　電子証明書の一時停止		
No.	相談内容	回答内容
1	電子証明書の一時停止・一時停止解除を導入することは可能でしょうか？	電子署名法上、証明書の一時停止、一時停止解除について規制している条項はなく、 認定認証事業者が運用規程（CP/CPS）において、「本認証局は、証明書の一時停止は行 わない」ことを規定しているものがほとんどであり、適切な運用規程を設けることで、 証明書の一時停止、一時停止解除を取り扱うことは可能だと考えます。 なお、RFC3647 での運用規程（CP/CPS）等の目次案では、 ・ 電子証明書一時停止の要件 ・ 電子証明書一時停止の請求者 ・ 電子証明書一時停止の請求手続き ・ 電子証明書一時停止の可能期間 等について、記載することを求めていますので、参考にしてください。 なお、「電子証明書の一時停止」の導入に関しましては、運用条件や、署名検証者側のシステム対応状況等についても十分ご確認の上、慎重に進めてください。 運用条件等が具体的になりましたら、改めてお問合せください。 【関係法令】
2	会員組織からの申請による電子証明書の一時停止・一時停止解除を導入することは可能でしょうか？	会員組織で運営されている認証局で、当該組織会員のみを利用対象者としている場合は、会員個人が会員組織から脱退した場合や会員資格を失った場合には、会員個人からの申請がなくても、会員組織からの申請により、当該電子証明書を失効させることは、予め運用規程（CP/CPS）や利用者規約等で規定しておけば、問題ないと考えます。「電子証明書一時停止」の扱いにつきましては、Q1 の回答を参考にしてください。 なお、「電子証明書の一時停止」の導入に関しまして

		は、運用条件や、署名検証者側のシステム対応状況等についても十分ご確認の上、慎重に進めてください。 【関係法令】
7. 業務体制		
No.	相談内容	回答内容
1	認証業務の運用体制の見直しとして、最小限の員数あるいは兼務等で業務を実施できるように運用体制を変更する場合は、変更認定の申請が必要でしょうか？	認証業務の作業要員を最小限の員数で実施するように変更する場合は、変更認定の申請は必要ありません。認証業務の作業要員が役割を兼務することで最小限の員数で実施する場合は、内部牽制等の機能を損なわないように変更する場合は、変更認定の申請は必要ありません。 【関係法令】 施行規則第六条第十五条ロ
2	認証局要員の最小数１名としているもの(責任者等)を正副２名体制に変更あるいは他の要員が代行できるように運用体制を見直すことは問題ないでしょうか？	要員が正副２名で運用する場合は、責任の所在を明らかにして下さい。緊急時の対応のために正副２名体制にする場合は、緊急となる場合を明らかにした上で、業務責任の範囲を明らかにして下さい。 また、他の要員が代行できるようにする場合は、事務取扱要領等の規程に代行業務を規定し、緊急時には他の役割と兼務で業務が実施できないことのないようにして下さい。 【関係法令】 施行規則第六条第十五条ロ 施行規則第六条第十五条ホ
8. 鍵更新		
No.	相談内容	回答内容
1	鍵更新の認定取得前に、新しい発行者署名符号の自己署名証明書および利用者電子証明書を検証システム側に提供することは可能でしょうか？	鍵更新調査時に指定調査機関の立ち会いの下で生成作成した新しい発行者署名符号、発行者電子証明書及びリンク証明書ペアについては、変更認定の取得を以て使用可能となります。変更認定の取得までの間は、誤った使用を含め安全に保存される必要があります。従って、新しい発行者電子証明書の外部への提供にあっては、変更認定の取得後に実施頂くことが望ましいものと考えます。

		また、機能検証用に使用する利用者の電子証明書についても、新しい発行者署名符号に更新した認証業務から正規に発行された利用者の電子証明書を提供して検証を実施していただく必要があります。この場合、正規に発行された利用者の電子証明書は、まさに正規の電子証明書でありますので、その取扱は、認証業務の運用規程（CP/CPS）に則って行われる必要がありますので、注意してください。 なお、以下の点については、遵守いただく必要があります。 ① 鍵更新に係る変更調査の場合も、通常の変更調査と同様、調査完了後は、調査実施前の状態で運用を継続し、認定を取得後に、当該変更を実施できることとなるので、鍵更新に係る変更認定を取得するまでは、旧鍵での運用を行う必要があり、認定を取得するまでの期間は、調査時に作成した発行者署名符号、発行者署名検証符号(発行者電子証明書)及びリンク証明書は、公開を含め使用することができないと解されます。従って、本件の場合も、認定を取得するまでは、新鍵に係る発行者電子証明書を検証システム側に提供することはできません。 ② 変更調査時に作成したテスト用利用者証明書は、発行した発行者証明書及び発行者署名符号の機能試験以外での利用は、認められませんので、調査完了前に全て失効されている必要があります。 【関係法令】 施行規則第六条第七号
2	鍵更新と同時に認証業務用設備の大規模な更改を実施することは、可能でしょうか？	鍵更新と同時に認証業務用設備の大規模な更改を同時に変更調査することは可能です。但し、変更調査の実施までに、大規模な更改内容についてその詳細を確認し、同時調査可能かどうかを判断することが必要になります。 【関係法令】
9. 業務廃止		
No.	相談内容	回答内容

1	業務廃止方法としては、どのような手順ですすめればよろしいでしょうか？	業務廃止にむけての事前調整 （１） 業務廃止に向けては、十分に余裕を持って、事前に主務省及び指定調査機関に、相談して下さい。 ･現在有効な電子証明書を所持する利用者へ、余分な負担や迷惑をかけないやり方で廃止スケジュールを検討して下さい。 例えば、全ての発行済電子証明書の有効期限満了後に、業務廃止を実施するようにして下さい。 （２） 利用者電子証明書の利用を確認した政府機関、自治体及びその他関連機関(BCA 等)へ事前に説明して下さい。 業務廃止時の留意点 （１） 業務廃止の周知 ･全ての事前調整終了後、社内決定し、速やかに主務大臣へ書面により届出を提出してください。主務省への廃止届けのコピーを指定調査機関にも提出をお願いします。 ･全ての事前調整終了後、社内決定し、利用者へ書面により周知を行って下さい。 ･全ての事前調整終了後、社内決定し、リポジトリ(Web 等）により社外へ公表して下さい。 （２） 利用者への業務廃止周知後の問合せ対応 ･更新利用を予定している利用者へ推奨事業者を提案して下さい。 ･現在の利用者に不安を与えない説明を準備して下さい。 ･対応者による説明の差異をなくすためのマニュアルを準備して下さい。 （３） 失効処理、CRL/ARL 等 ･自己署名証明書(新及び旧自己署名証明書)は、その後の検証ができなくなるため、失効しないで下さい。 ･業務廃止に伴う失効時にも利用者へ失効完了通知書を送付して下さい。

		･最後のCRL/ARL のnextUpdate は、当該最終CRL/ARL の公開を終了する日よりも先の日にして下さい。これは、公開中にnextUpdate を過ぎると、無効なCRL/ARL と判断されてしまうためです。 ･自己署名証明書(新及び旧自己署名証明書)については、最後のCRL/ARL の公開中は、現在と同様に掲載して下さい。 ･フィンガープリントについては、最後のCRL/ARL の公開中は、現在と同様の改ざん防止措置を維持した状態で公開して下さい （４） 帳簿書類の保存 ･適切な保存措置（漏えい、滅失又はき損防止措置）を施して保存すること。 ･1 年保存の帳簿書類については、保存は1 年でよく、廃棄時に廃棄の記録を残 すこと。 ･10 年保存の要件が課せられているもの(申込書類、規程類等)については、業務廃止後も施行規則第十二条第二項に基づき、引き続き保存するようにしてください。 ･利用者電子証明書、自己署名証明書、リンク証明書、相互認証証明書及びCRL/ARL 等を、電子データで保存する場合は、CD,DVD あるいは、DAT 等長期保存が可能で、読み出しに特別なソフトウェアを必要としないと思われる媒体で保存すること。 （５） その他 ･電子証明書発行受付終了日が決定したときは、その旨をCP、CPS 等の規程類に記載すること。 ･指針第十四条第四号に基づき、発行者書名符号（複製されたものを含む）について完全に廃棄すること。 【関係法令】 施行規則第十一条 指針第十二条第二項
10. その他 10.1 プロファイル		

No.	相談内容	回答内容
1	認証業務で使用している組織名として英語表記の略称を使用しておりますが、組織名の英語表記（フルネーム）に変更しても、運用規程（CP/CPS）における組織名の定義 を変更することで、継続して使用したいと考えておりますが、変更認定の申請が必要でしょうか？	電子証明書に記録しなくてはならない事項として、施行規則第六条第五号のイに「当該電子証明書の発行者の名称」が規定されています。したがって、組織名の英語表記としては、正式な根拠のある英語表記を電子証明書に記録すべきであると思料いたします。 貴認証局の現行の組織名は、組織名の英語表記（フルネーム）の略称を組織の意志決定機関の承認を受けて使用しており、英語表記（フルネーム）の変更後も“xxxxxxx”が組織名称の「呼称」であることを組織の意志決定機関にて正式に承認した上で、運用規程（CP/CPS）に定義するのであれば、引き続き電子証明書のissuer 及びsubject に記載する組織名(organizationalName)として“xxxxxxx”を使用することは、認定基準に適合するものと思料いたします。 また、貴認証局の英語表記についても、組織名の英語表記（フルネーム）を変更した 後も、現行のままで変更しないことを組織の意志決定機関にて正式に承認するのであれば、引き続き電子証明書のissuer 及びsubject に記載する組織単位名(organizationalUnitName)として “xxxxxxxxxxxxxxxxxxxCA”を使用することは、認定基準に適合するものと思料いたします。 変更認定の要否につきましては、今回のお問合せによる変更箇所が、運用規程（CP/CPS）で定義している組織名の「略称」を「呼称」とするだけであることから、電子署名法第四条第二項第三号の事項の変更には該当せず、変更認定の必要はないと思料いたします。実施に際しましては、変更に伴う規程改訂等の記録を残してください。 次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 【関係法令】 施行規則第六条第五号の
2.証明書プロファイルの変更について		
2-1	証明書プロファイルの属性情報	利用者証明書に記載されている利用者の氏名を除く

	（事務所所在地の都道府県、市区町村以下）を空白に変更して電子証明書を発行することは可能でしょうか？	属性情報（事務所所在地の都道府県、市区町村以下等）の証明を空白とすることは可能です。 利用者証明書が、「属性情報（事務所所在地の都道府県、市区町村以下）が記載されたもの」と「属性情報（事務所所在地の都道府県、市区町村以下）が空白のもの」の２種類が併存することになりますので、運用規程（CP/CPS）他関連規程に、次のことを明記してください。 a. 属性情報（事務所所在地の都道府県、市区町村以下）を、空白とした新たな利用者証明書への切り替え時期を明確にすること b. それ以前に発行された利用者証明書（属性情報（事務所所在地の都道府県、市区町村以下）が記載されているもの）は引き続き有効とするのであれば、以前の運用方式を継続（利用者証明書に記載された、いずれの属性情報が変更になっても失効させる）すること c. 利用者証明書のプロファイル等の記述は、２種類のものを併記する、及びその適用時期を明確にすること 【関係法令】 施行規則第六条第八号
2-2	証明書プロファイルの属性情報（事務所所在地の都道府県、市区町村以下）を空白にする場合、以下のいずれの運用が可能でしょうか？ １ 利用申込書に記載しないでよいとする。 ２ 利用申込書に記載させるが、郵便受領処理及び審査を行わないでよいとする。 ３ 利用申込書に記載させ、郵便受領処理を行うが、審査を行わないでよいとする。 ４ 利用申込書に記載させ、郵便受	利用申込書への記載方法、郵便受領処理及び審査の実施の有無につきましては、電子署名法上は、上記１乃至４のうち、いずれの運用でもかまいませんが、運用方法を検討されるに当たって配慮すべき事項を挙げておきますので、ご参考願います。 a. いろいろなケース分けをして人の判断を増やす等により人的ミスを誘発することのないよう配慮すること b. 空白扱いする属性情報について、利用申込書に記載させるが郵便受領処理や審査を行わない等により、利用者証明書の信頼を下げることにならないように配慮すること c. 空白扱いする属性情報について、利用申込書に記載させて、郵便受領処理や審査も行った場合には、名

	領処理及び審査を行った上で、空欄の取扱いをする。	簿の記載情報と差異があった場合に名簿への反映をどうするか等の問題が出るので考慮しておくこと d. 属性情報の扱いの変更に伴い、システムの動作確認（バックアップや復旧動作等も含め）を十分に実施すること 新たな運用方法が決定し、規程類の改訂案等ができましたら、確認させていただきますのでご連絡願います。 【関係法令】 施行規則第六条第八号
3	リンク証明書（New with Old）（Old with New）のプロファイルから「subject altname」の項目全体を削除する場合は、変更認定の申請が必要でしょうか？	電子署名法の認定基準において、リンク証明書（OldWithNew、NewWithOld）のプロファイルは明確に定められていません。お問合せ頂いた修正内容（「subject altname」の項目全体の削除）の場合は、変更認定の申請は必要ありません。認証局が旧世代のCAから新世代のCA に移行した際、利用者及び署名検証者が自身の電子証明書を正しく検証可能な状態であることを前提に認定認証業務においてプロファイルの修正の定義を行い、定義通りの電子証明書の発行を行うように実施して下さい。 修正された規程類については次回の更新調査時に確認します。 【関係法令】

10.2 リポジトリ

No.	相談内容	回答内容
1	リポジトリに他認証局リポジトリへのリフェラル設定を追加することは、問題がないでしょうか？	リポジトリへの設定を追加することは、電子署名法第四条第二項第三号の事項の変更には該当せず、変更認定の必要はありません。なお、実施されたリポジトリへの変更情報について、事後に御報告をお願いいたします。 【関係法令】 施行規則第六条第九号
2	一般認証サービスと認定認証業務	電子署名法第四条第二項第三号の事項の変更には該

	の証明書や失効リストの公開を共用リポジトリで運用する場合は、変更認定の申請が必要でしょうか？	当せず、変更認定の申請は必要あ りません。 施行規則第十二条第一項第四号ホの認証業務用設備及び第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 なお、リポジトリの共用に際しては、一般認証業務の運用・保守作業等により、特定認証業務用のLDAP の運用に影響が及ばないように、十分な配慮をお願いいたします。 お問い合わせいただいた範囲内であれば、電子署名法第四条第二項第三号の事項の変更には該当せず、変更認定の必要はないと思われます。施行規則第十二条第一項第四号ホの認証業務用設備及び第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成いただき、次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 なお、リポジトリの共用に際しては、一般認証業務の運用・保守作業等により、特定認証業務用のLDAP の運用に影響が及ばないように、十分な配慮をお願いいたします。 【関係法令】 施行規則第六条第九号
3	各種規定類やフィンガープリントなどのホームページの構造を変更することは、問題ないでしょうか？	ご提示頂きましたホームページの変更案は、情報公開Web サイトから利用者が必要な情報を容易に得られるよう改善されているように思料いたします。実施に際しましては、テスト等を十分実施し、利用者が容易に、確実に当該ホームページから必要な情報をたどれることを、確認してください。また、関連規程類の修正（修正がある場合）、作業記録等の作成を行い、次回の更新調査時に指定調査機関による確認を受けてください。 【関係法令】

10.3　業務運用者用電子証明書		
No.	相談内容	回答内容
1	業務運用者用電子証明書のプロダクトの変更する場合は、変更認定の申請が必要でしょうか？	業務運用者用電子証明書は、調査表の1222 項番及び1223 項番で、以下の設備間通信に関する各設備の誤認等防止に使用されています。 更新調査においては、指針第五条第二号に基づき、認証業務用設備が二以上の部分から構成される場合における設備の誤認等防止措置について、当該証明書や設備の措置状況を確認しています。また、当該証明書の発行手順も変更になることから、施行規則第六条第十五号イに基づき、業務運用者用電子証明書の発行手順の教育・訓練の実施状況につきましても、確認する必要があります。 したがいまして本件は、法第四条第二項第二号及び第三号の事項の変更に該当し、電子署名法第九条に従い、主務大臣の認定を受ける必要があると思料します。 【関係法令】 指針第五条第二号 指針第六条第一項第一号
2	業務運用者用電子証明書の格納媒体を2048bit 鍵長に対応した媒体に変更する場合は、変更認定の申請が必要でしょうか？	業務運用者用電子証明書に関して、今後実施が予定されている2048bit 鍵長への移行に備えて、先行して2048bit 鍵長に対応した格納媒体に変更することは、電子署名法第四条第二項第二号の事項の変更には該当せず、変更認定の必要はないと思われます。 実施に際しましては、認証業務用設備及び規則第四条各号の基準に適合するために必要な設備の維持管理に関する記録を作成していただき、実施後の各業務の最初の更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。 【関係法令】 指針第五条第二号 指針第六条第一項第一号
10.4　**利用者署名符号の交付**		
No.	相談内容	回答内容

1	発行局から登録局への郵便引受番号の連絡を電子メール等で送信することは、問題ないでしょうか？	IC カード等を利用者に安全に送付するため、本人限定受取郵便（特例型）を使用した証拠として、また、郵便事故等により、送付物の追跡を容易にするために必要な、郵便引受番号が記録された受領証（紙）を電子化する方法、受領証（紙）の電子化後の措置、及び、送付手段としてS/MIME を使用する際に暗号化とともに、送信者を特定し、改ざんをも防止する電子署名・電子証明書を付した形での通知を行って頂ければと考えます。 本件変更は、変更認定を取得する必要はないものと思料します。 なお、使用する電子証明書は認定認証業務で発行されたものが望ましいと考えますが、非認定認証業務から発行される電子証明書を用いる場合は、当該電子証明書の仕様もあわせてご提示下さい。 【関係法令】 施行規則第六条第三号
2	PIN 封筒自動封入封かん機の更改で、チェックリストの内容を一部改定する場合は、変更認定の申請が必要でしょうか？	「電子証明書発行チェックリスト」の変更を伴う自動封入封かん機への用紙のセットや精製水の確認等のチェック項目の追加に伴い、PIN の生成の方法や発送方法に変更は無く、規程にも変更が無い程度の変更であれば、変更認定の申請は必要ありません。 変更内容については変更箇所が分かるように記録に残して頂ければと考えます。変更後の実施記録等については次回の更新認定調査時に確認致します。なお実施にあたり十分教育訓練を実施し変更箇所の運用に支障の無いよう実施して頂ければと考えます。 【関係法令】 施行規則第六条第三号
3　施行規則第六条第三号に関する問い合わせ		
3-1	利用者署名符号を送付する場合、総務省が定義する「信書」として送付する必要がありますか？	利用者署名符号のような電磁的記録媒体のみを単体で送付することは、信書の送達にはあたらないと思料します。しかしながら、業務上利用者署名符号のみを単体で送付することは通常では想定できず、利用者という特定の受取人に差し出す趣旨が明かな文言が記

		載されている文書を利用者署名符号と共に同梱した場合には、郵便法及び信書便法に規定された「信書」に該当することが想定されます。従いまして信書に関する詳細につきましては、総務省が定めた「信書に該当する文書に関する指針」及び「「信書に該当する文書に関する指針(案)」に対する意見の概要」等と総務省の考え方を参考にしていただき、さらにご不明な点は送付内容を判断し、必要に応じて総合通信局または総務省（情報流通行政局郵政行政部郵便課）にお問合せいただければと考えます。 【関係法令】 施行規則第六条第三号
3-2	受取人確認配達サービス＜〇〇〇便＞を使用する場合、施行規則第六条第三号の条件を満たしているのでしょうか？ サービス名：受取人確認配達サービス＜〇〇〇便＞ 特長　：配達時、送り状に記載されている荷受人さまご本人の名前と住所を運転免許証など公的証書で確認し、事前登録いただいたパスワードと照合、もしくは公的証書の記号・番号、生年月日をカード決済端末機に入力して配達するサービスです。 ＜郵便局の本人限定受取郵便との差＞本人確認をする際は原則、写真付き公的証明書（運転免許書等）の提示１点が必要であるが、写真のついていない公的証明書（健康保険証や年金手帳等）の提示１点でも引き渡し可能。	本人限定受取郵便は、郵便事業株式会社が定めた内国郵便約款第5 章第10 節（第137 条～第139 条）に規定された郵便業務です。第137 条には、「名あて人の来店を待って」 とあり、お問い合わせの「受取人確認配達サービス」よりも厳しい条件が課せられています。同条第2 項により、「名あて人本人に配達すること」もできますが、その際の条件についても規定があります。同社の郵便業務は、郵便法の定めるところにより行われ（郵便法第二条）、約款を変更しようとする際は、総務大臣の認可を受ける必要があります（同第六十八条）。また、電子署名法施行規則第五条第一項第一号ハにも規定され、利用者の真偽確認の一つの方法として認められている手段でもあります。 本人限定受取郵便が日本郵政公社において取り扱われていた当時、基本型に加え特例型が追加された際に、当時の主務三省及び認定基準WG において、利用者署名符号は本人限定受取郵便にて送付する必要があること、及び、特例型が使用可能なパターンについて以下のように整理されました。 利用者署名符号(IC カード等)を郵送する場合は、本人限定受取郵便（基本型または特例型）で送付する必要がある。 ＰＩＮ(IC カードPIN やPKCS#12PIN)を郵送する場合は、本人限定受取郵便（基本型または特例型）または簡易書留で送付す

		る必要がある。 パターン① _ 利用者署名符号とＰＩＮ を同梱して本人に送付する場合は、本人限定受取郵便（基本型）に限る。 _ 利用者署名符号とＰＩＮ を同梱して本人限定受取郵便（基本型）の代人に送付することは認められない。 パターン② _ 利用者署名符号を本人限定受取郵便（基本型または特例型）で本人に送付し、PIN を簡易書留で本人に送付することは認められる。 _ 利用者署名符号を本人限定受取郵便（基本型または特例型）の代人に送付する場合は、PIN を本人限定受取郵便（基本型または特例型）または簡易書留で本人に別送する必要がある。 したがって、本人限定受取郵便と同等の本人確認方法及び受渡手段が実施されないと考えられる受取人確認配達サービス＜〇〇〇便＞は、規則第六条第三号が求める「当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法」に該当しないと思料します。 【関係法令】 施行規則第六条第三号
3-3	他にこの条件を満たすサービスとして、郵便局の本人限定受取郵便以外にあるのでしょうか？	施行規則第六条第三号を満たすこの他のサービスは、指定調査機関では把握しておりません。 【関係法令】 施行規則第六条第三号
10.5　その他		
No.	相談内容	回答内容
1	士業連合会は公的認証サービスで発行された証明書の失効情報の提供を受けることが出来る「署名検証者」になることが認められておりますが、提供された失効情報をもとに証明書の有効性について確認した結果を署名確認者（代理申	本件は、「公的個人認証サービス」の署名検証者に関する問合せであり、電子署名法関連法令の観点から回答する立場にはないと考えます。 【関係法令】

	請を行う士業個人等）に対して回答することが可能でしょうか？	

2.1.5 2.2.5 認定認証事業者からの問い合わせ Q&A（帳簿書類の保存場所編）

この問い合わせ Q&A は、問い合わせ分類⑤の帳簿書類の保存場所についてまとめたものです。

1. 新規の帳簿保管場所		
No.	相談内容	回答内容
1	帳簿保管場所を新規の場所に移転する場合は、変更認定の申請が必要でしょうか？	帳簿保管場所を移転する場合は、帳簿の保管場所の漏えい、滅失又はき損の防止のために必要な措置の調査を実施することが必要であり、変更認定の申請が必要となります。 現地調査時の確認事項としては、 ・室の扉、間仕切り ・室の自動火災報知器及び消火装置の設置(消火器、スプリンクラー等) ・直射日光に対する遮蔽措置 ・室、キャビネットの鍵（物理鍵や IC カード等）の管理方法 等になります。 【関係法令】 施行規則第六条第十五号ヘ
2	更新調査時に、帳簿の保管場所の追加調査を同時に実施して頂くことは可能でしょうか？	更新調査時に、新しく追加する帳簿の保管場所の漏えい、滅失又はき損の防止のために必要な措置の調査を同時に行い、認定を取得することは可能です。認定の更新後に、新しい帳簿の保管場所を利用することができるようになります。 現地調査時の確認事項としては、A1 の確認事項と同じ内容となります。 【関係法令】 施行規則第六条第十五号ヘ
2. 認定済みの帳簿保管場所について		
No.	相談内容	回答内容
1	認定を受けている帳簿の保管場所を認定の対象外とすることは、変更認定の申請が必要でしょうか？	保管場所を認定対象外とすることは、電子署名法第四条第二項第三号の事項の変更にはあたらず、変更認定の申請は必要ありません。

		実施に際しましては、保管場所の最後の利用の記録及び保管場所を廃止するときにその時点で保管物がないことを記録した作業記録を作成し、次回の更新調査時に指定調査機関による作業記録の確認を受けていただきますようお願いいたします。 【関係法令】 施行規則第六条第十五号へ
2	認定を取得している帳簿の保管場所内でキャビネット（金庫等）を移動することは、変更認定の申請が必要でしょうか？	認定を取得している帳簿の保管場所内で、キャビネット（金庫等）を移動させることは、電子署名法第四条第二項第三号の事項の変更にはあたらず、変更認定の申請は必要ありません。 当該内容に係る作業記録を作成し、変更後の更新調査時に指定調査機関による確認を受けていただきますようお願いします。 【関係法令】 施行規則第六条第十五号へ
3	認定を取得している帳簿の保管場所に、新たにキャビネットを追加することは、変更認定の申請が必要でしょうか？	認定を取得している帳簿の保管場所に、新たにキャビネットを追加することは、管理権限など帳簿書類の保管場所での鍵の管理等の変更がない場合には、電子署名法第四条第二項第三号の事項の変更にはあたらず、変更認定の申請は必要ありません。 ただし、認証設備室にキャビネットを追加する場合、キャビネットが地震等で転倒し、認証業務用設備を破損させることがないように措置することが必要となります。 当該内容に係る作業記録を作成し、変更後の更新調査時に指定調査機関による調査を受けていただきますようお願いします。 【関係法令】 施行規則第六条第十五号へ
4	認定を取得している別の保管場所へ保管物を移動することは、変更認定の申請が必要でしょうか？	帳簿書類保管場所として認定を受けている場所への帳簿書類の移動は、帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置、管理権限など

		帳簿書類の保管場所での鍵の管理等の変更がない場合には、電子署名法第四条第二項第三号の事項の変更にはあたらず、変更認定の申請は必要ありません。 もし、定期的に帳簿書類を移動するような場合については、移動に関する規定を作成し、移動の実施を記録する帳簿を作成し、実施するようにして下さい。 帳簿書類の移動を記録した作業記録を作成し、次回の更新調査時に指定調査機関による作業記録の確認を受けていただきますようお願いいたします。 【関係法令】 施行規則第六条第十五号へ
3. 帳簿の媒体変換について		
No.	相談内容	回答内容
1	原本を紙媒体の帳簿から電子媒体の帳簿に変更することは、変更認定の申請が必要でしょうか？	電子署名法の帳簿書類保存措置として、紙媒体で保存されている過去の資料(利用者またはその代理人の署名又は押印がない書類に限る)（施行規則第十二条第四項）を、電子媒体に格納されているデータに置き換えることは、紙媒体で保存されている情報と、電子媒体に格納されているデータの情報が同一であることが確認できれば可能となります。この保存媒体の変更は、紙媒体に記録された情報に対応する情報が確実に電子媒体に存在することが確認され、情報を保管している装置、環境条件等が規則第六条第十五号へに規定された措置を満たしており、情報が適切に保存されることが担保されれば、変更認定の申請は必要ありません。 但し、公的書類（住民票の写し、印鑑登録書等）については、偽造防止処理がなされた証明書等があり、スキャンされたデータを再生した場合、偽造防止処理による不必要な情報が混入することからスキャン対象とすることはできないものと考えます。 一方、保管場所については、施行規則第六条第十五号への措置を確認することが必要であり、認定を受けていない場所に電子データを保管しようとしている場合は、変更認定の申請が必要となります。 電子データをサーバ等に保存している場合、認証業務

		の要員以外からアクセスを禁止する措置がなされていることも確認することになります。 【関係法令】 施行規則第六条第十五号ヘ 施行規則第十二条第四項
2	電子データを保管しているサーバのハードウェアおよびソフトウェアの変更を予定していますが、保管するファイルへのアクセス制御には変更がない場合、変更認定の申請が必要でしょうか？	電子データを保管しているサーバの設置場所および管理方法に変更がなく、文書の保管環境およびアクセス制御等には変更がない場合、変更認定の申請は必要ありません。 【関係法令】 施行規則第六条第十五号ヘ
3	委託契約している会社が分割することになり、会社分割する前の委託契約書の代わりに、分割後に委託を承継する会社との委託契約書を原本とし、保管することで問題ないでしょうか？	契約書は、施行規則第十二条第一項第三号ニに規定されている帳簿書類で、施行規則第十二条第五項で「第一項各号に掲げる帳簿書類（前項に規定する書類を除く。）は、その原本を保存しなければならない。」と規定されており、契約時点で作成されたあるいは、使用された契約書の原本を保存する必要があります。また、施行規則第十二条第二項に「前項第一号から第三号までに掲げる帳簿書類は、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。」とされていますので、当該保存期間まで保存義務があることとなります。 分割後に承継する会社との委託契約についても、施行規則第十二条第一項第三号ニに規定されている帳簿書類となり、保存義務があり、更新調査時にその原本の存在、保存場所、保存状態及び保存環境を確認することとなります。 【関係法令】 施行規則第十二条 *補足
4. 業務廃止あるいは業務委託終了について		
No.	相談内容	回答内容
1	廃止済の認定認証業務の帳簿書類	電子署名法施行規則第十二条第二項に基づき「前項第

	（利用申込にかかる書類）は廃棄してよいでしょうか？	一号から第三号までに掲げる帳簿書類は、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」する必要があります。当該規定は係争等への対応を考慮し、定められています。
2	業務委託を終了する場合、業務委託先で保管していた帳簿書類は廃棄してよいでしょうか？	規則第十二条第一項第一号～第三号適用の帳簿書類は、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する義務があります。業務委託が終了しても、保存義務がある帳簿が委託先で保管している場合、委託元の更新調査時に委託先の帳簿保管状況を確認することになります。 委託先で保管していた帳簿書類を委託元の認定された保管場所に移動する場合は、更新調査で委託先の帳簿書類の保管状況を確認する必要がなくなります。 また、委託契約書は、更新調査時では委託元にある委託契約書を確認し、委託先で保管している委託契約書については確認しておりません。委託先で必要な期間、委託契約書を委託先で保管していても、委託契約書だけが保存されている場合は更新調査時に委託先を調査することはありません。 【関係法令】 施行規則第十二条

＊3 帳簿の媒体変換についての No.3 の補足【業務委託関連帳簿の保存】

認定認証事業者は、施行規則第十二条第一項／第二項に基づき、帳簿書類を保存する必要がありますが、業務委託関連で受託する側での契約書の扱いについては、一部異なる点があります。

	業務委託の契約書	
	委託側	受託側
保存義務	【保存期間】 ・規則第十二条第二項の適用（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）	【保存期間】 ・規則第十二条第二項の適用を受けない 【保存】

	【保存】 ・規則第六条第十五号へ に基づく漏えい、滅失又はき損防止に必要な措置	・規則第六条第十五号へ に基づく漏えい、滅失又はき損防止に必要な措置 （漏えい防止が主）
更新 調査時	・規則第六条第十五号へ に基づく措置を実地調査により確認	・規則第六条第十五号へ に基づく措置を実地調査により確認 （帳簿の保存ということより、記載内容の漏えい等の危険性に着目した調査であり、調査の程度が異なることがある）
保管場所の変更時	・保管場所の変更には、事前に変更調査の申請が必要 ・規則第六条第十五号へ に基づく措置を実地調査により確認	・保管場所を変更する場合は、委託元に通知する ・契約書の保存期間が満了し、廃棄しようとする場合は委託元に確認を行い、記録を残して廃棄

	施行規則第十二条第一項で規定される文書（契約書以外）	
	委託側	受託側
保存義務	【保存期間】 ・規則第十二条第一項の適用（対象帳簿書類） ・規則第十二条第二項の適用（保存期間） 第一項第一号～第三号の帳簿書類：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 第一項第四号の帳簿書類：作成した日から認定の更新の日まで 【保存】 ・規則第六条第十五号へ に基づく漏えい、滅失又はき損防止に必要な措置	
更新調査時	・保存対象の全帳簿書類について、規則第六条第十五号へ に基づく措置を実地調査により確認	
保管場所の変更時	・保管場所の変更には、事前に変更調査の申請が必要 ・規則第六条第十五号へ に基づく措置を実地調査により確認 ・保管場所を変更する場合は、委託元に通知する	

	・契約書の保存期間が満了し、廃棄しようとする場合は委託元に確認を行い、記録を残して廃棄

3. 情報提供

3.1 課題検討

運用上の課題やその検討結果、相談事項の概要等を報告書にまとめるとともに、相談に対する回答・助言等のうち、特に特定認証事業者等が共有すべき事項について取りまとめ、Web 等により情報提供を行った。

なお、報告書の作成、回答・助言等の実施及び特定認証事業者等が共有すべき事項の取りまとめにあたっては、指定調査機関としての調査業務実施経験から蓄積された知見を踏まえ、より総合的な検討を加えた。

3.1.1 (1) 課題検討

1) 課題の分類

特定認証業務の認定基準に関する課題について、表 3.1 の項目表に基づいて整理･検討した。

整理・検討した課題と、分類との対応は、次のとおりである。

- 電子署名・認証制度全般（No.1~5-3、21、22）
- 認証業務の用に供する設備（No.6、23）
- 利用者の真偽確認（No.8）
- 認証業務の実施方法（No.9~16、20~21）
- 帳簿保存（No.7、17~19）

また、表 3.1 の課題を、次の観点で表 3.2 ～表 3.4 にまとめた。

表 3.2： 特定認証事業者等が共有すべき事項および認定に係る調査業務を通じて把握される課題として整理したもの（表 3.1 の①に該当する項目）

表 3.3： 回答・助言等のうち、特に特定認証事業者等が共有すべき事項のとりまとめにあたり、指定調査機関としての調査業務実施経験から蓄積された知見を踏まえ、より総合的な検討を加えて整理したもの（表 3.1 の②に該当する項目）

表 3.4： 指定調査機関として認定に係る調査業務を実施する過程で把握される電子署名法運用上の諸々の課題を検討し、テーマにより特定認証事業者等および主務官庁殿と共有すべき事項を課題として、取りまとめたもの（表 3.1 の③に該当する項目）

表 3.1　項目表

No.	項目	①	②	③
1	運用による電子証明書発行対象に関する検討			○
2	属性情報の証明に関する検討		○	
3-1	署名符号の危殆化に関する検討（暗号アルゴリズム、発行者署名符号）			○
3-2	署名符号の危殆化に関する検討（利用者署名符号）			○
4	更新調査に関する検討			○
5-1	変更調査に関する検討（設備関連）	○		
5-2	変更調査に関する検討（真偽確認関連）	○		
5-3	変更調査に関する検討（業務運用関連）	○		
6	認証設備等に関する検討			○
7	電子申請に伴う電子保存に関する検討	○		
8	真偽確認方法に関する検討	○		
9	発行者署名符号・発行者電子証明書に関する検討	○		
10	電子証明書の記載事項に関する検討			○
11	安全な利用者秘密鍵取り扱いに関する検討			○
12	失効処理に関する検討	○		
13	有効期間が満了した失効情報の利用に関する検討			○
14	個人情報に関する検討		○	
15	認証業務運用者の権限に関する検討		○	
16	認証業務の業務委託に関する検討		○	
17	帳簿保存全般に関する検討	○		
18	設備関連の帳簿保存に関する検討			○
19	帳簿の電子化に関する検討	○		
20	電子証明書（利用者署名符号）の用途についての検討			○
21	認証業務の廃止に関する検討			○
22	指定調査機関の業務が不測の事態等により調査の実施、継続、あるいは期限内での完了が遂行できない場合に関する検討			○
23	認証設備室のパーテション上部の格子状の開口部に関する検討			○

2）特定認証事業者等が共有すべき事項の整理・検討および認定に係る調査業務を通じて把握される課題の整理・検討

特定認証事業者等が共有すべき事項および認定に係る調査業務を通じて把握される課題を

まとめたのが、表 3.2 の整理・検討結果１である。

表 3.2　　整理・検討結果１

No.	課題整理のポイント、検討内容、電子署名法関連部分
5-1	認定認証業務における変更申請が必要な事項に該当するかの判断基準について、施行規則に「(軽微な変更) 第九条　法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。」と規定しているが、その他の軽微な変更以外の要件の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 認証設備室、登録用端末設備が設置された室の変更 (2) 施設の軽微な変更の範囲 (3) 監視室移転 (4) 軽微な変更の規定のうち、「同一室内」が有効となる範囲 (5) 物理的セキュリティ装置の変更認定範囲 (6) 登録用端末設備を設置する室の移転に係る認証業務用設備の調査範囲 (7) 変更調査時の調査範囲に関して (8) 登録用端末設備の増減 (9) 変更調査手順に関して 【検討内容】 (1) 規則第九条の軽微な変更に関して、認証設備室及び登録端末設備室の変更認定要件を明確にすべきである。 現在までの事例は次である。 ・認証設備室の設置場所を変更した場合は、変更認定の必要がある。 ・認証設備室の設置場所は同じで、区画を拡縮した場合は、変更認定の必要がある。 ・登録用端末設備が設置された室の設置場所を変更した場合は、変更認定の必要がある。 ・登録用端末設備が設置された室の設置場所は同じで、区画を拡縮した場合は、主務省に確認してから判断する。 (2) 規則第四条第五号(参考；調査表項番 1500 番台)の措置内容を変更する場合、どの範囲までの変更が軽微として扱うべきか明確にする必要がある。またこのことは、保存帳簿の保存場所の措置等にも影響がある。 (3)指針第四条第一号ニに関して、遠隔監視等を行う監視室は、認証業務用設備が設置された室ではないので、電子署名法上の「室」の要件が適用されない。しかしながら、監視場所の移転に伴い移設される、不正なアクセス等を検知するシステム、モーションセンサー、監視カメラ、漏水センサー等の監視設備、監視方法、及び監視体制等の措置状況に変更が生ずる場合には、変更調査にて確認する必要がある。 また調査に伴い、監視業務の運用業務、及び認証業務に従事する者の責任と権限等に関する措置状況についても、その内容を確認する必要がある。 (4) 規則第九条では、「法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。」と規定されており、法第九条第一項では、第四条第二項第二号(申請に係る業務の用に供する設備の概要)となっている。しかし、規則第九条では「同一室内」という定義がなされているにも係らず、「室」に関する要件は、認証設備室及び登録用端末設備が設置され

	た室のみ規定されている。よって、軽微な変更の条件である「同一室内」は、認証業務用設備室内及び登録用端末設備が設置された室内に設置された設備のみが対象となり、それ以外の設備に関しては、「同一室内」という条件が定義されることは不自然であると思われる。 (5) 規則第九条の軽微な変更に関して、入退室管理装置や遠隔監視装置・映像記録装置は、どの範囲の変更が変更認定となるか。 例えば、入退室管理装置のバージョンアップに合わせて照合器が複数台から 1 台に構成変更となり、かつ、前室を廃止する等、全体の構成も見直され、モーションセンサの設定や電気錠の変更も行われるような場合、総合的なセキュリティ設定の確認を、実地調査で行った方が良いと思われる。 また、映像記録装置に関しては、製品の変更があった場合でもスペックの向上が認められる場合には、軽微な変更としても良いと思われる。 よって、認証業務設備以外の物理セキュリティ関連装置の変更認定要件を、明確にすべきである。例えば、単なるバージョンアップであるか否かを要件とするのではなく、現地調査を行った方が良い変更については、バージョンアップであっても変更の認定とすべきである。 (6) 法第九条の変更認定において RA 室を移転する場合、RA 系設備や IA への通信回線も現状のまま移設されることが多い。そのような場合には、新 RA 室の措置を調査することは必須であるが、RA 系設備や IA への接続回線に関して変更がない場合は現地調査は不要と思われる。また、既存の RA 系設備を新 RA 室に一時移設して変更に係る現地調査を行うとなると、既存の RA 系設備は認定を受けた認証業務用設備であるので、その取扱い(持ち運びも含めて)は厳重に行う必要があり、場合によっては移動中に、物理的・ソフト的な障害が発生してしまう可能性もあるので望ましいことではない。 (7) 法第九条の変更認定においては、変更調査時に、変更前の設備系に関する措置が正しく行われていたかについて、変更調査時点までの措置を確認した方が良い。また、そのときの調査対象を明確にしたい。なお、次回調査時に確認が可能な内容に関しては、次回調査時に実施する。 (8) 規則第九条の軽微な変更に関して、認証業務用設備の増加(例えば登録用端末設備の台数の増加や、CA サーバの予備機の追加等)に関しては、電子署名法にて既に規定されており、軽微な変更である。しかし、季節的な作業量の一時増加等に係り登録用端末設備を増加し、作業終了後は減少させることについて、一時的な増分に対する減少の範囲であれば、特例として軽微な変更とする。ただし、一時的に使用した設備に係る帳簿類は全て保存する必要がある。 (9) 法第九条の変更認定においては、変更認定においては、認定を受けるまで設備の変更を行ってはならないこと、また、変更した措置を現地調査することが必要である。 しかし、既に認定を受けている設備の変更を行う場合、それらの条件を充たすためには既存設備を運用しながら、新規に設備を用意する必要があり、現実的に対応することが困難な場合がある。 このような場合、次のような手順で変更調査の実施方法をとっても良いことが望ましい。 ①変更申請 ②変更内容について指定調査機関に図面等の詳細資料を提出してもらい、資料内容を確認し、主務省にご連絡/確認後、主務省より着工の内諾を行う。場合によってはこの段階で第 1 回目現地調査を行う。 ③変更工事の実施（セキュリティ面に細心の注意を払いながら行い、次に実施する現地調査結果によっては迅速に現状復帰可能な状態で工事を行う）

	④指定調査機関による現地調査 ⑤変更の認定 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第九条　等 （軽微な変更） 第九条　法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。
5-2	認定認証業務における変更申請が必要な事項に該当するかの判断基準について、電子署名法等に「（軽微な変更）第九条　法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。」に規定しているが、その他の軽微な変更以外の要件の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 手交等の取扱（電気通信回線を通じた申込方式の追加） (2) 外国人の追加 (3) 真偽確認資料の追加 (4) 真偽確認ＮＧ時の訂正方法 (5) 利用申込書の作成方法の追加 (6) 重要事項の説明方法の変更 【検討内容】 (1) 手交等の取扱 信書扱いの認可を受けた業者による申込書（信書）の送付は、郵送の場合と同等に見做し、受領することができる。 (2) 外国人の追加 住民票の写しに登録原票記載事項証明書を追加することは、業務手順の変更はないと判断できる。登録原票記載事項証明書に記載された通称名を電子証明書に記載することは、業務手順の変更となり、変更認定申請が必要である。 (3) 真偽確認資料の追加 利用者の真偽確認資料として、「住民票記載事項証明書」、「広域交付住民票」及び「登録原票の写し」を、「住民票の写し」及び「登録原票記載事項証明書」に準ずるものとして真偽確認資料に追加することは、施行規則第五条第一項により可能である。ただし、「住民票記載事項証明書」は、利用申込者の氏名、住所及び生年月日が記載されたものであること、「登録原票の写し」は認証ある写し（＝原本と相違ない旨を公証する文言及び市町村長の記名押印が付されたもの）であることが条件である。 (4) 真偽確認ＮＧ時の訂正方法 認証局による利用申込書の自署欄を除くすべての項目の記述（修正）について、利用申込者の記述（修正）承認の意思が確認できれば（自署、実印による押印等）、認められる。 (5) 利用申込書の作成方法の追加 申込書への署名もしくは実印押印確認等の申込書受理後の真偽確認手続きに変更がない場合においては、変更認定の申請の必要はないと考えられる。なお、更新時において、利用者情報をプレプリントする場合は、個人情報の扱いに関し、認証業務規程ならびに利用者への説明文書であらかじめ、その旨を明記し、利用者への周知が必要である。

	(6) 重要事項の説明方法の変更 重要事項が説明された文書の送付方法の変更について、重要事項の内容やその説明について利用者から、同意を求め、その確認行為に変更がないことであれば変更認定の申請の必要がないと考えられる。ただし、利用申し込みの前に、説明文書が確実にダウンロードされることを配慮する必要がある。 【電子署名法関連部分】 電子署名及び認証業務に関する法律第六条第一項第二号、第十一条 電子署名及び認証業務に関する法律施行規則第五条第一項第一号、同項第二号、第五条第二項、第六条第二号、第十二条第一項第一号イ、ロ、ハ、ニ、ホ、ヘ、第十二条第二項(10年保存)、第十二条第四項、同条第五項 電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針第九条一号、二号、三号、四号、五号
5-3	認定認証業務における変更申請が必要な事項に該当するかの判断基準について、電子署名法等に「(軽微な変更) 第九条　法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。」に規定しているが、その他の軽微な変更以外の要件の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 利用者署名符号に係る受領書の形式、受理方法の変更について (2) 認証局鍵更新、発行者署名符号、発行者電子証明書の更新について (3) 利用者署名符号の発送方法の変更または追加について (4) 失効情報の提供方法の変更または追加について (5) 電子証明書の記録事項の変更または追加について (6) 利用者署名符号生成場所の変更または追加について (7) 失効申請受付処理の変更または追加について 【検討内容】 (1) 利用者署名符号に係る受領書の形式、受理方法の変更について 受理方法を、紙による郵送からオンラインによる送信に変更する場合、利用者署名符号を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法(電子署名法施行規則第六条第三号) により行う必要があることから、変更認定が必要である。 (2) 認証局鍵更新、発行者署名符号、発行者電子証明書の更新について 発行者署名検証符号に係る電子証明書の値を SHA-1、SHA-256 等で変換した値 (フィンガープリント)によって認定認証業務を特定することが指針第十条第二号で定められていることから、発行者署名符号、発行者電子証明書の更新はフィンガープリントの変更となり、変更認定が必要である。 (3) 利用者署名符号の発送方法の変更または追加について 施行規則第六条第三号の規程により、利用者署名符号を安全かつ確実に利用者に渡すことができる方法について送達手段の安全性が下がることがないことを確認している。事前に安全性が下がることがないことを確認できれば、処理手順の変更内容により変更認定が必要かどうかに分かれる。 (4) 失効情報の提供方法の変更または追加について 署名検証者は、適切な手段により、電子証明書について失効に関する情報が記録されていないことを確認すべきであることが、指針第十一条第三号で定められているため、失効

	情報の提供方法の変更または追加が実施されることで、署名検証者への失効情報が適切に提供されることを確認する必要があることから、変更認定が必要である。 (5) 電子証明書の記録事項の変更または追加について 電子証明書の記録事項が変更、追加になることは変更認定の対象ではない。しかし当初より利用対象者が異なり、申し込み方法（真偽確認方法含む）も異なる場合、本来は、別の認証業務をたて、電子証明書を分けることが望ましいが、認証事業者の責任において同じ電子証明書を複数の目的で使用することは電子署名法上明確に制限してはいない。 (6) 利用者署名符号生成場所の変更または追加について 指定調査機関の調査に関する方針の第４ 認証業務の実施の方法２．の規程により、利用者署名符号の生成は、認証設備室内又は同等の安全性が確保できる環境で実施されなければならないことから、生成環境に変化が生じる場合は、その生成環境が認証設備室内又は同等の安全性が確保できる環境であるか確認する必要があるため、変更認定が必要である。 (7) 失効申請受付処理の変更または追加について 本人死亡時等の第三者申請の追加は、電子署名法の規定外なため、変更認定は不要だが、当該申請を受付ける行為は告示(指針) 第十二条第一項第六号の CPS における「電子証明書の失効に関する情報の確認の方法」の変更のため、変更認定が必要である。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第三号 電子署名及び認証業務に関する法律施行規則第六条第十号 電子署名及び認証業務に関する法律施行規則第六条第十五号へ
7	電子申請を受付ける場合の電子署名などの有効性確認方法、受信した電子文書をどのように帳簿書類として保存することについて、電子署名法、施行規則、指針に規定しているが、電子データの保存要件明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 電子署名法のこれまでの考え方の整理 (2) 電子署名付き文書の有効性確認方法や保存方法の標準的技術 (3) 過去の事例 ・過去の電子署名付き電子文書の有効性確認方法や保存方法の事例や問合せの状況はどうか。 ・認定認証業務の安全性・信頼性の観点から、どこまで基準要件とするか。 【検討内容】 (1) 電子署名法のこれまでの考え方の整理 ①電子文書による保存が規定されていたが、具体的な方法、要件については規定がなく、実運用上の判断基準が不明確。 ②指針第６条第１項第二号にある認証業務用設備を利用者情報及び利用者識別符号の識別によって自動的に作動させる方法が追加されたことで一気通貫で利用申請から電子証明書の発行まで行える仕組みがととのったが、実運用に至らない障害について整理する。 (2) 電子署名付き文書の有効性確認方法や保存方法の標準的技術 ① 電子署名付き文書の有効性確認方法 電子署名付き文書の有効性確認方法は、電子申請の事例を調査し、その仕様を確認することで、一般的な有効性確認方法を確認する。【事例案：地方公共団体における申請・届出等手続に関する汎用受付システムの基本仕様(第二版) (総務省)】

	② 電子文書の保存方法の標準的技術 　電子文書の保存に係る帳簿ごとに要件、例えば企業活動を行う上で作成する帳簿類は、これまで紙の状態で7年間保存することが義務付けられていた。電子帳簿保存法による電子文書の保存が出来る要件を整理する。（事例案：電子帳簿保存法要件） 　電子文書の原本性を確保維持する長期保存方法について、現状の技術とその実用性を調査する。 署名データフォーマット（CMS 署名、XML 署名、PDF 署名）、長期保存フォーマット、RFC3126ETSI「TS 101 733」CAdES、XAdES(ETSI TS 101 903) ECOM「電子文書の長期保存と見読性に関するガイドライン」参照 ECOM「電子文書の長期保存と見読性に関する報告書」参照 海外の事例 EU 署名指令の適格電子署名では、届出認証サービスプロバイダーは、5 年間の文書保存と5 年間の署名検証の要件がある。 ドイツの電子署名法では、35 年の文書保存と署名検証可能が義務付けられている。（電子文書長期保存に関する現状調査報告書） (3) 過去の事例 　受領書データを電子署名付き文書を受信し、電子署名と文書本文を確認し、その記録を電子データ(紙媒体)で保存している事業者が数社ある。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第十五号へ　等
8	認定認証業務の利用者の真偽の確認の方法について、施行規則に規定しているが、認定認証業務の運用における具体的な真偽確認方法の判断基準(実運用上支障なく、且つ信頼性を維持する妥当な措置)について明確化の課題整理を以下のように実施した。 【課題整理のポイント】 1．日本在住の日本人及び外国人の場合 (1) 真偽確認時の住所、氏名の誤字・俗字等の扱い 　利用申込書の利用申込者の住所、氏名の文字が、住民票の写しに記載された文字と異なる場合、誤字・俗字を正字に置き換える判断基準が必要になることについて (2) 真偽確認時の外国人のローマ字表記 　日本人ならびに外国人の氏名の読みに関する規定がないことから、氏名の読み(ローマ字表記)の真正性に係る判断基準が必要になることについて (3) 真偽確認時の住所表示 　町名の字、地割等の固有名詞の扱い、建物名の記載の有無の扱い、住所、建物名の拗音、促音の扱い等に係る判断基準が必要になることについて (4) 真偽確認資料の有効期限 　真偽確認資料の内容の信頼性について、発行日からの有効期限を設けることに係る判断基準が必要になることについて (5) 真偽確認資料の返却 　利用の申込みを利用者の都合及び当該認証業務で利用者が求める電子証明書を発行することが困難な場合等により利用の申し込みを取り止める場合、提出された真偽確認資料の返却に係る判断基準が必要になることについて (6) 電子証明書の記載文字 　利用の申込みに係る真偽の確認が行われた後、電子証明書に利用者の氏名や住所を記録する場合、汎用的に使用するシステムの文字コードの制限により、同一の文字が表示できない恐れがある場合、誤字・俗字を正字に置き換える判断基準が必要になることについて 2．外国在住の外国人の場合

	(1) 真偽確認時の住所、氏名の確認方法 (2) 電子証明書の記載文字 3. 商業登記をしていない個人事業主の場合 (1) 事業を営んでいることを証明する書類 (2) 真偽確認時の氏名、申請事業所等の名称(屋号)、住所の確認 【検討内容】 1. 日本在住の日本人及び外国人の場合 (1) 真偽確認時の住所、氏名の誤字・俗字等の扱い 現在の認証事業者の扱いについて、利用の申し込みは、住民票の記載どおりに記載させ、一致を確認後、誤字俗字・正字一覧表等を用いて、電子証明書への記載文字を決定するか、Web申し込み時に利用者が JIS 第一・第二水準に置き換えて申し込みを行い、認証事業者が審査時に住民票との差異を誤字俗字・正字一覧表等で置き換えの妥当性を確認し、電子証明書には、置き換えたものを記載すること。 (2) 真偽確認時の外国人のローマ字表記 日本人ならびに外国人の氏名の読みに関する電子署名法上の規定はないことから、記載された氏名の読み(ローマ字表記)の真正性は、認証事業者の判断に委ねられている。外国人については、事例発生の都度、方向性・考え方(パスポート、辞典等による判断規定等の例示)の指導等により規定がなされ、実質的な対応のばらつきは殆ど見られない。しかしながら、日本人については、氏名に難解な漢字又は読み方を使用するケースが増えてきたにもかかわらず、その真正性の確認方法を規定している認証事業者がないことから、人名事典、健康保険証、パスポート等により真正性を確認する旨を規定し、実施する必要がある。表記方式については、一部事業者を除き、ヘボン式を採用している例が多い。 (3) 真偽確認時の住所表示 住民票に建物名の記載がない場合があることについては、各市町村が「街区方式による住居表示の実施基準」(昭和 38 年7月 30 日自治省告示第 117 号。以下「基準」という。)に沿って事務処理を行っているためであると考えられる。 すなわち、基準においては、中高層建物について、建物の道路への主要な出入口の基礎番号と各戸の番号を合わせて住居番号とすることとされている。この場合、住居表示は、 ○○県○○市○○△丁目△番◆－★号(◆:基礎番号、★:各戸の番号)となる。したがって、中高層建物については、住民票に建物名の記載がない場合がむしろ通常であると考えられる。 また、住民票の写しに建物名/部屋番号等が記載されない場合において、利用申込者も建物名、部屋番号を省略した場合、真偽確認上は、内容の一致で問題はないが、建物名、部屋番号がないと郵便が配達されないケースがあり、郵送先を確認する方法について明確にしておく必要があり、例えば、公的あるいは公共機関が発行/送付した書類等で、日常的に郵便が配達されている住所(建物名/部屋番号付)が確認できるものを確証として提示してもらうことがよい。 利用申込書と公的書類の住所表記は完全一致が原則であるが、住所表記に差異がある場合で、同一の住所と認められる事項について、主務省と確認が取れているのは以下のもののみである。 ①公的書類の「1 丁目 2 番 3 号」と利用申込書の「1-2-3」は同一と見なす。 ②公的書類に方書き(建物名、マンション名等)の記載がなく、利用申込書に記載がある場合は同一と見なす。だだし、この逆の公的書類に方書きの記載があり、利用申込書に記載がない場合は、同一と見なさない。 ③「ヶ(サイズ小)」と「ケ(サイズ大)」は、同一と見なす。 (例)三ヶ日 ⇔ 三ケ日 ④「○○番地●」と「○○番地の●」は、自治体から発行される「住民票の写し」等に「地番の後の「の」表示の有無は区別していない」旨が記載されている場合は同一と見なす。

	⑤丁目、番、号の「アラビア数字」を「漢数字」に、「漢数字」を「アラビア数字」に置き換えて表記することは、同一と見なす。 なお、上記以外の例外事項については、指定調査機関において今後再検討し、有識者及び主務省に相談の上、その結果を全ての認定認証事業者へ周知し統一する必要がある。 (4) 真偽確認資料の有効期限 商業登記において求められる、自治体が発行する代表者の印鑑登録証明書の有効期限は、発行日から3ヶ月以内と規定されているが、電子署名法では、真偽確認資料の有効期限について、住民票の写し等の証明書類の発行日についての要件は定められていないものの、現状においては、その有効期限は、全ての事業者で発行日から3ヶ月以内としている。 (5) 真偽確認資料の返却 真偽確認が完了する前においては、利用申込者の真偽確認以外の相当の理由(例えば、入札利用等の差し迫った利用者の要求する期限までに、電子証明書を発行できない場合や当て字を用いないため外字を持つ人には証明書を発行できないといった制約等)により利用申込みを承諾しなかった場合、または、利用申込者が当該相当理由(人事異動で不要になった等)により申し込みを取り下げた場合を前提に、住民票の写し等の真偽の確認を行う帳簿書類を返却することは、規程類を整備し、実施することは差し支えないと判断している。 (6) 電子証明書の記載文字 現状の誤字・俗字の電子証明書への記載実施状況は、申込書に、住民票どおりの記載を求め、真偽確認を済ませた上で、電子証明書記載に当たって、住民票の住所、氏名にJIS第一・第二水準以外の文字が有る場合は、認証事業者が誤字俗字・正字一覧表等を用いて、JIS 第一・第二水準内の正字に置き換えるか、置き換えが不可能な場合は、「カナ」または「ひらかな」に置き換えて、電子証明書に記載するか、Web 申し込み時に利用者に当該文字を JIS 第一・第二水準に置き換えて申し込みをしてもらい、認証事業者が審査時に住民票との差異を誤字俗字・正字一覧表等で置き換えの妥当性を確認し、真偽確認を行い、その記録を残す。また、電子証明書には、置き換えたものを記載する。等の対処がなされている。 2. 外国在住の外国人の場合 (1) 真偽確認時の住所、氏名の確認方法 住民票の写しに代わるものとして、戸籍(韓国、台湾、中国)あるいは、外国人の本国の公的機関が発行したパスポート, 国籍証明書等の身分証明書, 身分登録簿の写し, 出生証明書(いずれも, 日本語訳の添付が必要。)などが考えられるが、更なる検討が必要である。 (2) 電子証明書の記載文字 検討中。 3. 商業登記をしていない個人事業主の場合 (1) 事業を営んでいることを証明する書類 ・「一般建設業の許可について(通知)」は、都道府県により、記載内容(氏名、申請事業所等の名称(屋号)及び同住所)が異なることが実地調査時に確認された。(例) 大阪府の場合は氏名、申請事業所等の名称(屋号)及び同住所を記載。群馬県の場合は、住所が記載されない。 ・「個人事業の開・廃業届」は、開業届を市町村役場に提出した時期と電子証明書発行申込時期とに隔たりが大きい場合、事業所等住所が変更になっていることがあり注意が必要である。 (2) 真偽確認時の氏名、申請事業所等の名称(屋号)、住所の確認 認証事業者は、事業を営んでいることを証明する書類の記載内容、形式、直近に発行されたものであることを確認し、事業を営んでいることを証明する書類と利用申込書に記載された氏名、申請事業所等の名称(屋号)及び同住所が一致していることで真偽確認を行う必要がある。

	なお、複数の事業を営んでいることを証明する書類による真偽確認でも問題ないが、規程類に規定し、実施する必要がある。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第五条 電子署名及び認証業務に関する法律施行規則第六条第二号 電子署名及び認証業務に関する法律施行規則第九条　等
9	認定認証業務に係る発行者署名符号（認証局秘密鍵）及び発行者電子証明書の更新や暗号モジュールについて、施行規則、指針に規定しているが、認定基準要件及び調査対象の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 鍵更新等の措置に関連し、要件の追加(変更認定、旧鍵の破棄タイミングの明確化等)が必要 (2) 発行者署名符号の復元に係る措置要件について (3) 署名検証者に対する説明事項について、旧発行者電子証明書と新発行者電子証明書とのつながりの維持、それに係る一定期間発行するリンク証明書についても、署名検証者が必要に応じ入手することが可能な措置がなされることが必要。 (4) 発行者署名符号の作成又は管理に係る電子計算機(暗号装置)について、JCMVP での暗号装置の認定との連携を模索することについて 【検討内容】 (1) 鍵更新により新発行者署名符号が生成された後、旧発行者署名符号の不正使用が起こらないように、廃棄タイミングについて規定することが望ましいと思われる。指針第十四条第四号では、「発行者署名符号の使用を終了する場合には、複数の者により物理的な破壊又は完全な初期化等の方法により完全に廃棄し、・・・」と規定されているが、この「使用を終了する場合」ということが、各事業者の解釈がまちまちであり、新鍵生成直後に廃棄する事業者もあれば、認証局電子証明書の有効期間内は残すという事業者もある。また、「認証局電子証明書の有効期限を越して発行者署名符号を残してはいけない」ということについても、実際に認証業務アプリケーションの仕様上不可欠であるとの理由で鍵更新による新鍵の使用後も、旧発行者署名符号を使用不可能な状態で保存している所もあり、署名法上の規定化を実施することについては難しいと考える。 発行者署名符号を更新せずに新規に作成した場合（新鍵に重なることなく旧鍵を破棄)、新規認定の必要性を再検討する。特に危殆化時のコンティンジェンシープランとの関係で、全認定認証業務をいかに速やかに移行させるかについて、慎重に議論を重ねる必要がある。 (2) 発行者署名符号の復元操作に関して、指針第十四条第二号ロに「(発行者署名符号を再生する場合には･･･)」という規定があるにも関わらず、調査表の該当する適合例(3E2X)には「復元」がないので、追加することが望ましい。 (3) 認証局鍵更新においても認証局鍵の生成、認証局電子証明書及びリンク証明書の作成を行うことから、調査表の該当する適合例（351X）に、リンク証明書(ペア)のフィンガープリントの記録と公開を、追加することが望ましい。 (4) 2009 年 11 月 9 日、2 回目のドラフト版（Revised DRAFT）の FIPS140-3 が発表されている。2007 年 7 月のドラフト版では、LEVEL５が登場していたが、最新のドラフト版では FIPS140-2 同様に LEVEL４に戻された。パブコメは 2010 年 3 月 11 日に締め切られている。NIST の Web ページ(http://csrc.nist.gov/groups/ST/FIPS140_3/index.html)によると、次回のパブコメの開始は未定とされている。FIPS140-2 との差異や、最新のドラフトに対

	するコメントによりどのような点がさらに修正されるか、施行規則第四条第四号への影響範囲を検証する必要がある。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第四条第四号 電子署名及び認証業務に関する法律施行規則第六条第十七号 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十四条第一号 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十四条第四号　等 （関連する規程） 電子署名及び認証業務に関する法律施行規則第六条第六号 電子署名及び認証業務に関する法律施行規則第六条第九号 電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針第２の２．暗号装置関係
12	認定認証業務で発行する電子証明書の失効処理を行う場合について、施行規則に規定しているが、失効処理作業の実施に係る要件（失効申請者の定義と本人確認、認証局事由の失効と電子証明書の再発行、認証局事由と失効通知、失効通知方法、失効処理における遅滞ない時期）について、より明確化するための課題整理を以下のように実施した。 【課題整理のポイント】 運用上、要件を整えることが必要な措置について、以下のとおり規準をより明確化することが必要と思われる。 (1) 失効申請者の定義と本人確認についての、失効申請者の範囲と利用者との関係の確認基準について (2) 認証局事由の失効と電子証明書の再発行について、認証局事由による失効の取り扱い、誤発行並びに電子証明書格納媒体（IC カード等）不良等による電子証明書の再発行の手続き（二重発行の防止）について (3) 利用申請者や代行申請者並びに親族等の申請時における失効通知先について (4) 施行規則第六条第十号に規定する遅滞なく電子証明書の失効することに係る遅滞無く実施する期間について (5) 施行規則第六条第十二号に規定する電子証明書の失効に関する情報を記録した場合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について 【検討内容】 (1) 失効申請者の定義と本人確認 属性認証を含め、失効申請者の範囲やその資格要件が明確にされておらず、認証事業者の判断に委ねられている。また、失効申請を利用者以外のものを含める場合、利用者と失効申請者の関係を明確にする方法等の基準がなく、認証事業者の判断に委ねられている。 (2) 認証局事由の失効と電子証明書の再発行 誤発行並びに IC カード不良等の電子証明書の再発行については、再発行時における、真偽確認資料等の扱いが問題となるが、再発行事由や発行からの再発行までの期間ならびに当初発行した証明書から、5 年を越えない場合等を考慮し、再提出は、不要としている例が多い。 (3) 失効通知先等 利用申請者や代行申請者（親族等の申請を含む）の申請時における失効通知先ならびに

	通知の有無等については、現実的な処理を行っている。認証局事由による場合も、利用者に電子証明書が渡っていない場合は、失効通知を利用者に送付しない等の処理を行っている。 (4) 遅滞なく電子証明書の失効することに係る遅滞無く実施する期間について 遅滞無くとはどの程度の期間を表すかの判断基準は、明確に示されていないが、受理後から、一営業日との認識だが、商慣習及び業界ルール等により必ずしも同一の解釈を得ることが難しいが、文字通り、「処理をとどめないとの範囲」でと考えている。 (5) 電子証明書の失効に関する情報を記録した場合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について 権利能力は出生によって始まり、死亡によって終わることが相続の開始を規定した民法第 882 条からすると、利用者死亡の場合は、死亡によって、自然人の権利能力が消滅するため、利用者への通知義務は必須ではないこととなる。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第十号 電子署名及び認証業務に関する法律施行規則第六条第十一号 電子署名及び認証業務に関する法律施行規則第六条第十二号　等
17	認定認証業務に係る保存帳簿書類の分類、保存期間、保存条件、保存場所の見直しについて、他法律の帳簿の保存期間と電子署名法の帳簿の保存期間の扱いについて明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 保存期間 施行規則第十二条により、帳簿書類は「認証事業者の組織管理に関する帳簿書類」及び「設備及び安全対策措置に関する帳簿書類」に分類され、前者は、電子証明書の有効期間の満了日から 10 年間の保存義務、後者は、作成した日から認定の更新の日まで保存する義務を負う。この保存期間と、他の法律で規定された保存期間との違いに係る認証事業者の管理の混乱を防ぐため、適正な保存期間、帳簿書類ごとに保存義務の差別化を検討。 契約書等については、税法等の保存期間と電子署名法の保存期間に差異があり、保存期間を短くすることの是非について検討。 (2) 保存場所 施行規則第六条第十五号へにより、利用者の真偽の確認に際して知り得た情報の目的外使用の禁止及び第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置として、帳簿書類の保存が求められることに対する漏えい、滅失又はき損の防止の定義の検討 帳簿書類を保存している事務所等の移転に伴って、帳簿書類の保存場所が変更になる場合等、認証業務と無関係な要因によって保存場所を変更することとなった場合の保存場所の変更タイミングについて、また帳場書類の保存場所は、その環境条件、運用条件が施行規則第十二条に要求されている条件を満たしていることの確認方法について (3) 保存条件 施行規則第六条第十五号へにより、第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置が求められる帳簿について、CPS や利用申込書等の公開文書と事務取扱要領等内部規程の非公開文書において、帳簿書類の記載内容の漏えい、滅失又はき損の防止のレベルについて検討。 【検討内容】 (1) 保存期間 現在、電子署名法で保存を要求している帳簿書類の中でその保存期間を他の法律等で規

	定しているものとしては、契約書が確認されている。その他の帳簿書類については、こうした条件があるものは確認されていない。 ・契約書については、税法等で、各種の規定があり、2 年から永年までが規定されているが、委託契約で関係するものは、通常の契約行為であることから契約書の保存期間が 7 年(契約書のとらえ方により必ずしも 7 年とは限らない)とされている。これらの契約書は、通常、契約担当部門が契約の実施、検収管理、保存管理、等の全てを実施することが社内で規定されていることが多く、認証業務の担当部門が保管について管理できないし、していないのが実状であり、このため、各事業者から、契約書の保存は、他の業務の契約書と同じ取扱をさせていただきたいとの要望が出ている。特に、大手ベンダー等が、その子会社を再委託先とした場合、各契約書は、子会社との間で結ばれている包括的な契約(基本契約)に基づいて、部門間での契約として通常注文書等の形態を取っている。これらの契約書は、通常、契約期間が満了し、経理、税務関係の処理が完了すると一纏めとして保存する例が多く、その保管方法、管理方法、等において、漏えい、滅失又はき損防止のための措置を取っているとの確認を実施していない場所となることがある。 ・基本契約では、個々の業務契約に共通な事項のみが規定されており、電子署名法で要求している「委託業務の内容、委託元の指示の遵守、責任分担と保証等」についての記載はない。したがって、これらの事項は、部門間で実施される注文書に記載するか、別途、その内容を仕様書に記載する等の措置が採られている。さらに、一部では、部門間で実施される注文書による契約を電子契約により実施しており、 帳簿保存対象が電子データとなっている例がある。この場合、電子契約システムは、汎用的に構成されていることから、契約書を含む、関係情報の保存期限を 7 年とし、その後の保存措置は考慮されていない場合がある。 (2)保存場所 　現在使用中の保存場所がオーバーフローする等により保存場所を追加、変更する場合、その場所の調査を更新調査時に実施する確認によってすませる場合がある。これは、Q&A73 に基づいて実施しているものである。この場合の報告は、当該更新認定調査に係る事前報告時に確認した旨を説明書に記載することですませ、報告の形態を取っていなかったため、このように、変更認定として実施した場合と、更新認定に合わせた場合で、一方は、調査報告書が提出され、他方は、正式な記録が無いという差異が出るのは、余り良いとはいえないと思われることから、更新認定で実施している調査を変更認定調査と位置付け、更新調査報告時に更新調査報告書に調査状況を併記し、報告する方法を導入した。調査手数料については、更新調査時に帳簿書類の保存場所の追加等に係る調査を同時に実施した場合の手数料を追加する（旅費等については、更新認定と一体として請求することにより事業者の負担を軽減できる。）。 (3)保存条件 　施行規則第十二条の帳簿・書類の中で以下の通り予め利用申込者及び署名検証者その他のものが閲覧することを目的とする公開帳簿として ・利用者への説明用書類（利用者同意書、説明事項同意書　等） ・利用の申込書に関する書類（利用申込書原紙　等） ・発行者電子証明書または発行者署名検証符号 ・失効の請求書（電子証明書失効請求書原紙　等） ・認証業務規程（CP、CPS） 利用申込者及び署名検証者その他のものが閲覧することを認めない非公開の帳簿として ・利用申込書、失効請求書等 ・真偽確認の提出書類（住民票の写し、印鑑登録証明書　等） ・申込み諾否を決定した者の氏名及び承認しなかった理由を記載した帳簿（電子証明書発行指示書　等） ・電子証明書の発行管理簿

	・発行者電子証明書または発行者署名検証符号、及び作成記録 ・利用者署名符号生成・廃棄に係る帳簿（利用者署名符号生成・廃棄管理簿　等） ・失効の判断に関する記録 ・業務手順の変更記録 ・業務責任などの変更記録 等である。 公開帳簿は主に公開リポジトリに載せているが、公開文書なので、帳簿書類の記載内容の漏えいに当たる事項が見当たらないと思われる。滅失については、公開リポジトリにはオリジナルではなくあくまでコピーを載せるため、滅失してもオリジナルデータから容易に、直ちに復元可能である。き損の防止については、公開リポジトリサーバの取扱、バックアップデータの存在等を調査時に契約書や規程類で確認すべきである。 非公開帳簿が、電子データとして保存されている場合については、非権限者に見られる(漏えい）ことやき損の防止、滅失の防止について、また、公開帳簿のオリジナルの電子データを保存するサーバ等を外部ネットワークからの脅威を抑えるための FW の設置やサーバ本体へのアクセス制限措置、RAID 構成としての障害対応などが実施されていることを調査時に確認すべきである。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第十五号へ 電子署名及び認証業務に関する法律施行規則第十二条　等
19	認定認証業務に係る紙の帳簿書類の電子化保存について、要件の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 真偽確認資料等の紙の申請書類等をスキャナで電子化した帳簿書類の保存に係る方式の基準等について、紙媒体の帳簿書類の電子化保存の基準(発行申請書等の有印文書、公的証明書(コピーガードの有無による取扱を含む）)の明確化の検討 (2) スキャンによって帳簿書類とする電子データについて スキャンによって帳簿書類とする電子データについて、スキャンに伴う技術的要件の基準が必要であることについて (3) 有印文書、公的証明書等の原本要求の場合、施行規則第十二条第五項によりスキャンが認められていない。今後 e-文書法によって有印帳簿書類の電子化基準、偽造防止処理がなされた証明書等の電子化基準について 【検討内容】 (1) 真偽確認資料等の紙の申請書類等をスキャナで電子化した帳簿書類の保存に係る方式の基準等について 電子申請に係る電子データによる申請書類の作成基準(本人による作成の証明、作成時点での実在性の確認基準等)及び認証局における真偽確認等の証明、真偽確認後の保存に係る実在性の確認基準と、長期保存機能に係る要件(ハードウェア、保存方式、バックアップを含む長期保存基準、サーバ設置基準、運用基準、媒体変換に係る基準、等及び使用するタイムスタンプの要件(方式、有効期間、タイム精度、運用要件等)を含む)の明確化。 電子申請に係る電子データによる申請書類の作成基準としては、電子申請書等の当該帳簿書類が、申請者本人による作成であることが証明されること、非改ざんであることを証明できること、並びに、作成時点での実在性及び作成後における非改ざんの証明ができる必要があるものと考えられる。このため、電子申請書等の当該帳簿書類が、申請者本人による作成であることが証明されること、非改ざんであることを目的として、電子申請書等へは当該認証局が発行した有効な電子証明書に係る利用者署名符号もしくは、公的個人認証証明書に係る本人の署名符号によって署名が為される必要があり、その上で、作成時点での実在性、並びに、作成後における非改ざんの証明を目的として、対象情報を包含したタ

	イムスタンプが付与されることが必要であると考える。この時使用されるタイムスタンプは、十分信頼性があり、かつ、長期間の保存に耐える得るものであることが望ましく、現在、(財)日本データ通信協会が認定業務を実施している「タイムビジネス信頼・安心認定制度」の認定を取得しているものである必要があるものと考える。なお、電子申請に係る通信路での情報の漏えいを防止する措置、並びに、通信の相手を認証する機能を有するものである必要があり、SSL(クライアント認証)、IPVPN(アプリケーションでの通信相手の認証機能が必要)等の通信路の暗号化機能、並びに、認証機能を持った方法によって保護が為される必要がある。 (2)スキャンによって帳簿書類とする電子データについて 紙媒体の帳簿書類の電子化保存の基準(発行申請書等の有印文書、公的証明書(コピーガードの有無による取扱を含む)、スキャンにおける要件、長期保存機能に係る要件等)の明確化 ・スキャンによって電子データとすることができるデータについて、スキャンに伴う技術的問題等から基準を設ける必要がある。 (3) 有印文書、公的証明書等の原本要求の場合 有印文書、公的証明書等の原本を提出することとしているものについては、現在、施行規則第十二条第五項によりスキャンが認められていない。しかし、e-文書法によってスキャンが認められていることから、これらの帳簿書類のスキャンデータによる長期保存の要望は高まるものと考えられる。有印帳簿書類の電子化基準、偽造防止処理がなされた証明書等の電子化基準について検討する必要があるものと考える。 基本的には、有印文書(公的証明書を含む)は、スキャン対象としてもよいものと考える。しかし、偽造防止処理がなされた証明書等については、スキャンされたデータを再生した場合、偽造防止処理による不必要な情報が混入することからスキャン対象とすることはできないものと考える。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第十二条第四項 電子署名及び認証業務に関する法律施行規則第十二条第五項　等

3) 特定認証事業者等が共有すべき事項の取りまとめに対する課題の整理・検討結果

回答・助言等のうち、特に特定認証事業者等が共有すべき事項のとりまとめにあたり、指定調査機関としての調査業務実施経験から蓄積された知見を踏まえ、より総合的な検討を加えて整理したのが、表 3.3 の整理・検討結果２である。

表 3.3　整理・検討結果２

No.	課題整理のポイント、検討内容、電子署名法関連部分
2	認定対象外である属性情報の真偽確認方法や電子証明書への属性情報の記載について、施行規則、指針に規定しているが、電子証明書への記載する属性情報の真偽確認方法（根拠資料）及び指定調査機関として調査範囲に関する課題整理を以下のように実施した。 【課題整理のポイント】 (1) 属性情報の真偽確認方法 施行規則第六条第八号に規定する電子証明書に利用者の役職名その他の利用者の属性を認定認証業務に係るものであると誤認することを防止として、電子署名法の認定対象外とす

	ることの是非について、法令との関係と属性情報の真偽の確認方法を明確化することが必要と思われる。 (2) 指定調査機関としての調査根拠 【検討内容】 (1) 属性情報の真偽確認方法 証明書に記載する内容については、真偽確認で確認した属性情報に加えて、事業者独自の所属証明書、法に裏づけされた会員管理団体から発行された資格証明書等の提示を求める、または会員管理団体への資格の問合せ等を規定し、その内容を電子証明書に記載している。 (2) 調査時の確認事項 属性情報は、電子署名法の対象外との前提があるにもかかわらず、認定認証業務で発行されている電子証明書のアプリケーション事例で、圧倒的に使用されている官公庁や自治体における電子入札対応や企業間の契約取引対応のため、何らかの形態で属性情報（企業コード、社名等）を電子証明書に記載するサービスを実施している。 属性情報の誤認防止が関係規程類（CPS,利用規約等）に規定されていることの確認、及び、属性情報について、利用者から、提出された登記事項証明書や所属証明書、資格証明書等の形式、記載内容及び有効期間を確認すると共に利用申込書に記載された属性情報が提出された資料の属性情報と一致しているかを確認、また、発行された電子証明書のプロファイルを求め、プロファイルに申込どおりの記載がなされているかを確認している。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第八号 なお、規定されていないが、関係すると思われるものとして以下がある。 電子署名及び認証業務に関する法律施行規則第五条第一項第一号 電子署名及び認証業務に関する法律施行規則第六条第五号 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九条　等
14	認定認証業務に係る個人情報の取り扱いについて、個人情報保護法の規定（権利又は利益を侵害され、又は侵害されるおそれがある場合の開示申請の取扱について、また利用者の真偽の確認に際して知り得た情報の目的外使用の禁止について、または帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置について）と電子署名法の要件の差異について明らかにし、取扱について明確化にする課題整理を以下のように実施した。 【課題整理のポイント】 (1) 開示申請 権利又は利益を侵害され、又は侵害されるおそれがある場合の開示申請は、申出する際の必要書類と申し出方法、申し出を受理した時の真偽の確認方法、開示する情報について明確化する (2) 利用者の真偽の確認に際して知り得た情報の目的外使用の禁止 利用者の真偽の確認に際して知り得た情報の目的外使用の禁止は、個人情報の取扱及び保護に関して規定する。また利用者より提出される個人情報の適切な管理、電子証明書への記載範囲、また役割に応じた教育・訓練計画を策定し実施することについて (3) 帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置 帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置として、個人情報の取扱場所の基準と保管場所の整備基準。または電子証明書への記載範囲の明確化及び利用者への明示方法について　等 【検討内容】 (1) 開示申請

	施行規則第六条第十四号では、開示請求において規定すべき内容が明確になっていないことにより、CPS における開示範囲、内容、開示の方法等において規定が不明確であったり、不十分となっていたりしている例が出ており、これに対処するため、④については検討が必要である。 ① 申出する際の必要書類と申出方法(手数料を徴収する場合は手数料の額) ② 申出を受理した時の真偽の確認方法 ③ 開示する情報(当該電子証明書利用申込書類及び利用者の真偽を確認した資料、失効請求書類、電子証明書記載データ等) ④ 開示の方法 (2) 利用者の真偽の確認に際して知り得た情報の目的外使用の禁止 施行規則第六条第十五号へ　に規定する利用者の真偽の確認に際して知り得た情報の目的外使用の禁止に関する目的外の基準の明確化。 目的外となるものを規定することは困難であるので、使用目的を規定し、それ以外を特別な理由(司法からの要求等)がない限り禁止とする旨の規定をすることを求めるのが現実的である。使用目的として、当該認証業務のサービスを提供するために必要となる連絡等、利用者証明書の更新に係る案内等、当該認証業務に関連する情報等の案内等、並びに、それらに準ずるものとする。 (3) 帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置 ① 個人情報の取扱場所の基準と保管場所の整備基準。 個人情報の取扱場所としては、当該認証業務の担当者のみが入室できる場所であり、担当者等以外の入室が制限されるとともに､操作者の手元及び画面が覗かれない環境とする。他業務と共通の場所とする場合は、他業務への漏洩がないようにする措置(時間を分ける、帳簿書類の保存場所を完全に分け、当該業務担当者のみがアクセス可能とする措置を講じる等)が講じられる必要がある。 個人情報の保管場所としては、調査表 3C56 に示された条件を満たす場所であり、当該認証業務の担当者のみがアクセス可能な場所(専用キャビネット、専用保管室等であり、関係者以外からの攻撃を受けにくい場所(当該認証業務専用の部屋等))とする必要がある。 ② 電子証明書への記載範囲の明確化及び利用者への明示方法 申込書等の申込書類から電子証明書への記載範囲等について、その記載場所、記載方法等の規定がなく､利用者への説明についても不十分となっているものと思われることから、CPS、利用規約等における記載場所の明確化が必要と思われる。CPS においては、真偽確認基準及び真偽確認資料を説明した章、もしくは、条文に記載することとし、どの資料のどの事項が電子証明書のどの事項として転記されるのかを明確に記述する必要があると考えるので、この旨を調査表 3C53 に記述することがよいと考える。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第十四号 電子署名及び認証業務に関する法律施行規則第六条第十五号へ　等
15	認定認証業務に必要な役割とその責任及び権限（特に内部牽制や役割の兼務）に関する基準の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 認証業務に従事する者の責任及び権限並びに指揮命令系統及びその変更について全体的な安全性・信頼性の確保する観点で要件を明確化することについて (2) 要員の配置基準における適材適所的な要員配置について、電子署名技術、鍵管理技術、セキュリティ技術等に関する業務遂行上に必要な知識、経験それらを有している技術者の必要数を配置することについて

	【検討内容】 (1) 認証業務実施に必要な役割とその責任及び権限を明確にする上での基準 認証局において、セキュリティ確保の観点から、役割を定め、その役割での実施できる業務を規定し、責任と義務を明確にするとともに、権限を制限している。一方、認証局においては、運用者をできるだけ削減し、業務効率を高めたいという要求がある。しかし、要員の削減に伴って、RA 業務の運用者が IA 業務の運用者を兼務した場合、容易に不正を行うことができる環境ができてしまう場合が考えられることとなる。このような任用は、安全性、信頼性(セキュリティ)の確保の観点から絶対に避けるべきであり、その旨を、事務取扱要領に規定し、厳格に実施されるべきと考える。上記は、一例であり、それぞれの認証業務での実態に鑑みて、兼務に係る任用に関する規定がなされるべきである。 基準としては、認証業務の実施において、複数の役割における権限を兼務により複数取得した場合、不正行為の実施の可能性を大幅に増大させる任用の禁止を明確に定めることである。 認証業務における一般的な役割とその責任及び権限については、十分に一般的な考えが浸透しており、基準を示す必要はないものと考えるが、認証業務の構成及び実施範囲によっては、思わぬセキュリティホールが発生する場合があるので、内部牽制の実現、並びに、同一人物が入室できる範囲と設備を操作できる範囲等を勘案して役割毎の責任及び権限を設定するように注意を喚起する。 (2) 要員の配置基準における適材適所的な要員配置について 認証業務の実施において、複数の役割における権限を兼務により複数取得した場合、不正行為の実施の可能性を大幅に増大させる任用の禁止を明確に定めることである。 兼務を禁止する役割の例を、以下に示す。 ・登録業務における審査担当者と審査結果承認者あるいは、承認担当者(例、登録審査担当者と登録承認者) ・登録業務における審査担当者及び審査結果承認者あるいは、承認担当者と発行業務システム操作者等、利用者証明書の発行、失効等に係る操作を制御できる役割 ・セキュリティ管理者は、可能であれば独立した役割とし、業務のセキュリティについて客観的に評価、確認できるように、その責任及び権限を設定する。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第十五号ロ 電子署名及び認証業務に関する法律施行規則第六条第十五号ホ　等
16	認定認証業務に係る業務委託について、業務委託の実施、契約の内容の変更、委託契約における報告の取扱、業務委託会社の合併・分割・社名変更等の取扱等(施行規則第 6 条第十五号ハ)の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 業務委託契約の新規実施、委託業務内容の変更に係る取扱 (2) 業務委託を実施している会社の合併・分割・社名変更の扱い (3) 業務委託を実施している会社の変更の扱い (4) 業務委託に係る報告書の取り扱いと、報告の周期 (5) 業務委託の変更に係る委託元(認定認証事業者)の承認 (6) 委託契約の変更に係る確認の申請と報告義務 (7) 派遣者の任用基準の明確化 (8) 業務委託の範囲の明確化 【検討内容】

	(1) 業務委託契約の新規実施、委託業務内容の変更に係る取扱 ･業務委託を全く実施していなかった場合(業務委託を受けていた受託者が業務の再委託を全く実施していなかった場合を含む)に、業務委託し、新たに認証局要員を任命するのであれば(建物、電源設備、建物警備等は除く)、認定の変更を必要とする。 ・実施している委託業務の内容を変更する場合であって、その業務の一部または全部の業務委託を中止し、委託者自身が実施する場合及び業務委託先を別の会社等に変更する場合であり、業務の用に供する設備、利用者の真偽の確認、申請に係る業務に変更がなく、実地調査対象が実地調査済みの対象と全く同一である場合は、認定の変更は不要とする。 ・同一の業務委託先であっても、変更により業務の用に供する設備、利用者の真偽の確認、申請に係る業務の一部もしくは、全部が変更される、もしくは、実地調査対象が実地調査済みの対象と異なることとなった場合は、認定の変更を必要とする。 (2) 業務委託を実施している会社の合併・分割・社名変更の扱い 業務委託を実施している会社の社名変更及び合併・分割において、存続会社、もしくは、業務を引き継いだ会社が実施する業務に係る実地調査対象が、実地調査済みの対象と全く同一であり、業務の実施場所、環境、人員管理方法等の変更がない場合は、認定の変更は不要とする。 これらについては、Q&A72 及び 77 で整理されており、当該変更がこの整理に該当するかを事前に指定調査期間において確認し、指導してきている。 (3) 業務委託を実施している会社の変更の扱い 業務委託を実施している会社を変更する場合、実施する業務に係る実地調査対象が、実地調査済みの対象と全く同一であり、業務の実施場所、環境、人員管理方法等の変更がない場合は、認定の変更は不要とする。 (4) 業務委託に係る報告書の取り扱いと、報告の周期 報告は、委託業務が安全かつ、確実に行われていることを委託者が確認するためのものであり、必要な情報が適切な形で含まれている必要があるとともに、委託している業務の確認を行うのに適した期間毎に求められ、確認されるべきものである。期間については、業務内容によりいろいろであると考えられるが、業務の重要性に応じて定められることが原則である。しかし、極端に短いあるいは、長い設定は、業務の効率、認定期間との関連からも不適切であると考えられる。業務内容毎に、基準を設けることが望ましいと思われるが、それぞれの委託条件が異なることから、特別な場合を除き、毎月から四半期毎の範囲になるものと考える。 (5) 業務委託の変更に係る委託元(認定認証事業者)の承認 業務の委託元が業務の実施者(実施会社)を知らないと言うことは許されることではないので、委託契約等において、委託先が再委託を新たに行う、変更する、委託内容の重大な変更を行う等の場合、業務の委託元(認定認証事業者)の事前承認等を必要とすることを明確にしておくことが必要であると考える。 (6) 委託契約の変更に係る確認の申請と報告義務 業務委託については、かなりの部分が認定の変更を行う必要はないとしているが、これを野放しにしておくと、委託関係が管理されない状況に陥る危険性がある。また、基準の誤認、誤解釈により、本来、認定の変更が必要であったのにもかかわらず、認定の変更を受けることなく変更が実施されてしまう危険性がある。このため、これら契約の変更については、変更を実施する前に、指定調査機関にその詳細を提示し、確認を受けてから実施することと考える。 (7) 派遣者の任用基準

	認定認証業務の実施にあたり、外部より要員の派遣を求めて必要要員を確保する例があるが、この場合、業務実施者の全てを派遣者で賄うことは、業務上の責任を不明確としてしまう可能性があり、避ける必要がある。また、業務責任者を派遣者で賄うことについても同様な問題を生じやすいことから避けることが望ましいと考える。この考えから、派遣者での実施が可能な役割を明確にすることが望ましいと考える。 (8) 業務委託の範囲 認定認証業務の事業者が業務委託をできる範囲について明確にする必要がある。これまでの例では、認定を取得した事業者が業務の主体者となり、名目上、業務を推進するとしているが、その実は、業務の全てを別の事業者に委託しようという認定申請の例があった。これでは、業務の実施者が誰であるか不明確となり、事故が発生した場合の対応等に問題が発生するものと考えられ、現在は、このような形態の業務は認定されていない。 また、認定認証業務事業者は、業務の内、少なくとも、登録業務、発行業務の全て、もしくは、主要な一部(登録業務では、本人確認業務等、発行業務では、発行者署名符号の管理業務等)を実施する必要があることも合わせて規定することが望ましいと考える。としてきたが、士業の認証局で負担が大きいことから、既存の認定認証業務に士業向けの電子証明書発行サービスを新規タイプの追加とし、その認定認証事業者から登録業務を委託を受けて実施したいとの問い合わせがあり、外部有識者への意見聴取及び主務官庁への確認を行い、民間認証局から士業向けの電子証明書の登録業務の一部を委託業務として実施することは、発行責任が民間認証局であり、最終的な発行承認も民間認証局が行う場合においては、電子署名法上の問題はないものとの判断となった。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第十五号ハ 電子署名及び認証業務に関する法律施行規則第十二条第一項第三号ニ　等

4) 認定に係る調査業務を通じて把握される課題の整理・検討結果

指定調査機関として認定に係る調査業務を実施する過程で把握される電子署名法運用上の諸々の課題を検討し、テーマにより特定認証事業者等および主務官庁殿と共有すべき事項を課題として、取りまとめたのが、表 3.4 の整理・検討結果３である。

表 3.4　整理・検討結果３

No.	課題整理のポイント、検討内容、電子署名法関連部分
1	認定認証業務で使用する認証業務用設備以外の関連設備にどこまで当該認証業務の電子署名を使用できるかについて、施行規則第六条第七号、指針第十条の内容「当該認証業務の維持管理のために必要な場合における使用（指針第十条第一号ロ)」の適合例項番 3512「⑤当該認証業務用設備およびそれを操作する者に対して発行する電子証明書への電子署名」に規定しているが、電子署名の対象の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 施行規則第六条第七号に規定する「利用者その他の者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」として、当該認証業務の維持管理のために必要な場合に係る認証業務の運用のための電子証明書の使用について、利用可能な範囲をより明確化することが必要と思われる。

	【検討内容】 　他の認定認証業務との間の相互認証証明書への電子署名については、事例はない。 当該認証業務の維持管理のために必要な場合における使用(指針第十条第一号ロ)については、主に以下のような用途で使用されている。 ・ログ署名用証明書への電子署名 ・登録用端末設備と RA サーバ、IA サーバ間の中間に位置する通信用の証明書への電子署名 ・運用のための電子証明書の作成権限認証用の証明書への電子署名 ・ディレクトリサーバ証明書認証用の証明書への電子署名　等 これらは、指針にもある当該認証業務の維持管理に不可欠なものであるため、これらの証明書は既に認めている。 また、適合例項番 3512⑦の電子証明書失効情報および当該認証業務に関する情報等を開示する設備に対して発行する電子証明書への電子署名からは、公開リポジトリサーバに対して電子証明書を発行できると解釈できる。しかし現在は、指針第十条第一号ロ「当該認証業務の維持管理のために必要な場合における使用」を前提としているため、公開リポジトリの内部向け認証に使用する電子証明書に用いることとしており、外部に対する公開リポジトリを認証する SSL サーバ証明書の事例はない。 【電子署名法関連部分】 (1) 電子署名及び認証業務に関する法律施行規則第六条第七号「認証業務に関し、利用者その他の者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ていること。」 (2) 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十条第一号「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。ただし、次に掲げる場合を除く。(指針第十条第一号) イ　他の認定認証業務その他認定認証業務と同程度以上の基準に従って国又は地方公共団体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（指針第十条第一号イ） ロ　当該認証業務の維持管理のために必要な場合における使用（指針第十条第一号ロ)」 (3) 適合例項番 3512 発行者署名符号の用途は認証業務の発行する電子証明書への電子署名のみに使用される。 上記以外に発行者署名符号を使用する場合は、以下の項目内に限定される。 ① 他の認定認証業務その他認定認証業務と同程度以上の基準に従って国又は地方公共団体等が実施する認証業務との相互認証証明書への電子署名 ② 当該認証業務の電子証明書への電子署名（自己署名） ③ 当該発行者署名符号の更新処理のため､新しい当該認証業務の電子証明書への電子署名 ④ 当該発行者署名符号の更新処理のため、古い当該認証業務の電子証明書への電子署名 ⑤ 当該認証業務用設備およびそれを操作する者に対して発行する電子証明書への電子署名 ⑥ 電磁的に記録する失効に関する情報への電子署名 ⑦ 電子証明書失効情報および当該認証業務に関する情報等を開示する設備に対して発行する電子証明書への電子署名
3-1	認定認証業務で使用する暗号アルゴリズムの危殆化(又は危殆化したおそれがある場合)、及び発行者署名符号自体の危殆化(又は危殆化したおそれがある場合）について、指針等に規定しているが、危殆化の判断または対処方法等の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 危殆化事象の分類と影響範囲の調査と検討 　電子署名アルゴリズム、公開鍵暗号アルゴリズム、ハッシュ関数アルゴリズムについて、

	それぞれの危殆化時の脆弱性を調べ、影響範囲を検討する。 (2) 危殆化回避方法の調査 　現在問題視されているハッシュ関数アルゴリズムの危殆化の回避方法について調べる。 (3) 認証局側(HSM、CA アプリケーション等)、利用者側、検証者側及び利用アプリケーションの SHA-2 化対応可能状況の調査 (4) 危殆化の判断と、対応方法及び制約 危殆化による移行判断の検討と、危殆化対応方法の検討 (5) 新暗号アルゴリズムを用いた環境への移行 (6) 暗号危殆化時の緊急時対応計画(コンティンジェンシープラン)のモデル案の作成 【検討内容】 (1) 危殆化事象の分類と影響範囲の調査と検討 　電子署名アルゴリズム、公開鍵暗号アルゴリズム、ハッシュ関数アルゴリズムについて、それぞれの危殆化時の脆弱性を調べ、影響範囲を検討する。 ・公開鍵暗号アルゴリズムの危殆化とその脆弱性の影響範囲 ・ハッシュ関数アルゴリズムの危殆化とその脆弱性の影響範囲 ・電子署名アルゴリズムの危殆化とその脆弱性の影響範囲 ・設備間認証、通信等に使用する場合、署名用途（文章等への署名、認証時の署名）での脆弱性の違い (2) 危殆化回避方法の調査 現在問題視されているハッシュ関数アルゴリズムの危殆化の回避方法について調べる。 ・SHA-1 から SHA-2 への移行 ・RSA1024 から RSA2048 への移行 ・他のハッシュ関数 ・暗号アルゴリズム、計算困難性（bit 数)、実装、その他の危殆化回避方法 なお、移行時期に関しては GPKI は 2014 年度末では新アルゴリズムに移行を完了する予定である。発行者署名符号を更新した場合はその時点から現アルゴリズムでの新規発行は不可能となる。認定認証業務の CA 証明書及び利用者証明書に関しても、2014 年度末に発行を停止するように現在検討が進んでいる。 (3) 製品、サービスの調査　　関連製品、関連サービスの対応状況について調べる。 ・認証局側 SHA-2 化対応可能状況(HSM、CA アプリケーション) ・利用アプリケーションの SHA-2 化対応可能状況(IC カード、USB トークン、クライアント OS、メーラ、ワープロソフト、PDF、ブラウザ、利用者作成アプリケーション（入札システム、申請システム、認証システム等)、リンク証明書の検証) ・GPKI,LGPKI の対応状況 ・その他(通信システム、暗号ライブラリ（MS クリプト API、PKCS、Java、OpenSSL、Web サーバ、LDAP 製品、他) ・利用者側 SHA-2 化対応可能状況 ・検証者側 SHA-2 化対応可能状況 (4) 危殆化の判断と、対応方法及び制約 危殆化による移行判断の検討と、危殆化対応方法の検討。なお、対応するために、制約条件の洗い出しも行う。 ・電子署名法及び認証局における SHA-1 危殆化の判断（CRYPTREC、「電子政府推奨暗号リスト」参照等）と、移行方法、及び移行における制約事項の洗い出し ・電子署名法及び認証局における発行者署名符号の危殆化の判断と、判断点以前の利用者の電子署名の有効性について。発行者署名符号更新時も含む。 ・発行者署名符号の危殆化の判断と、判断点以前の利用者の電子署名の有効性について。発行者署名符号更新時も含む。

	・利用者署名符号の危殆化の判断と、判断点以前の利用者の電子署名の有効性について ・発行者署名符号の危殆化前の移行について、その方法の検討（鍵更新を含む)、ハッシュ更新、タイムスタンプの利用（長期署名） ・利用者署名符号の危殆化前の移行について （移行方法、手順の検討（鍵の再利用の可否、新規鍵の生成措置確認、新旧鍵のリンクの可否、旧 CA の措置、新 CA の認定、署名検証者への情報提供、他） ・電子政府推奨暗号の安全性、実装性の評価等を行っている「暗号技術検討会」や、電子署名法附則第３条に基づき検討を行った「電子署名及び認証業務に関する法律の施行状況に係る検討会報告書」において、電子署名等のために広く使用している暗号アルゴリズム SHA-1 及び RSA1024 の安全性が低下しているとの指摘がなされ、それらを踏まえて H21 度「電子署名法における暗号アルゴリズム移行研究会」が開催された。 (5) 新暗号アルゴリズムを用いた環境への移行 ・暗号アルゴリズムの移行に伴い、2014 年度早期（X-day）以降、電子署名法に基づく認定認証業務は、新暗号アルゴリズム（SHA-2 及び RSA2048）による電子証明書の発行を開始し、現行暗号アルゴリズム（SHA-1 及び RSA1024）による電子証明書については、新規発行を停止し、発効済みの電子証明書の検証のみとする必要がある。そのため、X-day に向て、電子入札コアシステムにおいては、新暗号アルゴリズムで発行した認定認証業務の電子証明書に対応できるように署名検証環境の整備を着実に進める必要がある。 ・GPKI は 2014 年度末では新アルゴリズムに移行を完了する予定である。 (6) 暗号危殆化時の緊急時対応計画(コンティンジェンシープラン)のモデル案の作成 緊急時対応計画の雛型は以下の方針で作成されているので、方針に従ってモデル案を作成した。 ・緊急時対応計画は出来るだけシンプルにする ・他の規定を引用できる箇所は出来るだけ引用を用い、記述を少なくする ・緊急時対応計画は変更可能なように、改訂のプロセスを明記する ・回復手順（新暗号アルゴリズムへの移行、再発行）に関しては、発動後の回復手順の決定方法、決定後の主務省への報告内容を必須とし、回復手順自体の記述はオプション扱いとする ・緊急時対応計画の実施時、事後に主務省への報告は必要だが、責任者の判断で緊急時対応計画に盛り込まれた内容以外の対処を可能とする 【電子署名法関連部分】 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三条 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十条第二号、電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針第４９等
3-2	利用者署名符号が危殆化、又は危殆化する恐れがあることについて、危殆化の考え方を整理する課題整理を以下のように実施した。 【検討内容】 (1) 法律上の危殆化の定義 (2) 利用者以外の者に利用者署名符号が渡ったケースについて (3) 法律上の利用者の定義 【電子署名法関連部分】 (1) 法律上の危殆化の定義 電子署名法及び関連法令では、利用者署名符号の危殆化に関する規定は、以下のとおりである。

	①「危殆化の定義」：指針第八条第三号 ②「利用者署名符号の危殆化」：指針第八条第三号 危殆化とは、「盗難、漏えい等により他人によって使用され得る状態になることをいう」 (2) 利用者以外の者に利用者署名符号が渡ったケースについて 電子署名法第 2 条において、本人だけが行うことができるものである状態以外の状態になる時、他人により使用され得る可能性が出て来た時点で危殆化の恐れが発生すると考えられる。 認定基準を検討する平成 12 年 9 月 6 日（水）〔郵政省電気通信局会議室（9 階 S2)〕「認定基準等ワーキンググループ」第 3 回会合において、利用者本人の秘密鍵を利用者が管理外の企業等のサーバに置くことの是非について、電子署名法制定時に議論された推定効に関する議論の紹介がなされた。その議論の経緯から考えると、本人性の推定が働きにくくなるような「電子署名」を認めることは現時点では困難であるとしている。 (3) 法律上の利用者の定義 電子署名法第二条の定義のより「自らが行う電子署名についてその業務を利用する者」としている。 【電子署名法関連部分】 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八条第三号
4	認定認証業務における更新調査に関する課題整理を以下のように実施した。 【課題整理のポイント】 (1) 認定の有効期間と認定調査の実施間隔について (2) 認定の有効期間と認定調査の実施時期について 【検討内容】 (1) 認定の有効期間と認定調査の実施間隔について 現行では更新期間は 1 年。また認定の更新の手続及び基準については、第四条第二項（認定の手続）、第五条（欠格事由）及び第六条（認定の基準）が準用されるため認定の更新の際の手続及び基準は、認定と同じである。 (2) 認定の有効期間と認定調査の実施時期について 電子署名及び認証業務に関する法律施行令第一条に「認定の有効期間は 1 年とする」と規定してあるが、1 年の範囲であれば、更新時期は、事業者から申請があった場合変更が可能であるとの見解があり、これまでに変更実績がある。 【電子署名法関連部分】 電子署名及び認証業務に関する法律第七条 電子署名及び認証業務に関する法律施行令第一条　等
6	設備関連の基準要件において、より具体的に規定すべき事項やセキュリティ技術の進展により見直すべき事項が課題提起されていることについて、課題整理を以下のように実施した。 【課題整理のポイント】 (1) 認証設備室の変更（認証設備室の壁の取り外しを含む）に伴う、工事期間中の認証設備室への入出場管理の措置及び非権限者による認証業務用設備の作動防止等セキュリティ対策について (2) 認証設備室と「同等」の要件の明確化に係る、具体的には認証設備室と同等の安全性

	を明確化することについて (3) 指紋認証装置の脆弱性について　生体認証への認証要素の追加 　生体認証装置のうち、生体データの他に1要素、例えばパスワードやICカード併用してセキュリティの向上を図ることについて (4) 建築関連の法規が改正等により調査表適合例とあわなくなっているか、また影響を与えているかの調査について (5) 防火区画の確認図面について事業者提出の図面の信ぴょう性 【検討内容】 (1) 認証設備室の工事等が発生した場合、その間、認証設備室への入出場を管理するための措置（施行規則第四条第一号）及び正当な権限を有しない者による認証業務用設備の作動を防止するための措置（施行規則第四条第三号）に相当するセキュリティ対策が取られるので、問題ないという主務省のご判断をいただいている。 (2) 指針第十四条第二号イでは「認証設備室内で規則第四条第四号に規定する専用の電子計算機を用いて行われ、かつ、複製されたバックアップ用の発行者署名符号は、認証設備室と同等の安全性を有する場所に保存されること。」と規定されているが、「認証設備室と同等の安全性」とは具体的にどの要件を満たせばよいかについては、認証設備室とほぼ同じ要件で調査を実施している。 (3) 指針第四条で規定されている生体認証装置のうち、指紋認証装置等については指紋の複製が可能であるとの識者の意見があるので、認証情報として入力するデータは、生体データの他に1要素加えることが望ましい。 (4) 建築基準法（平成23年12月24日改正）には、第2条9の2で耐火建築物、第2条9の3で準耐火建築物、第20条で構造耐力がそれぞれ規定されており、法の改正後においても調査表適合例との乖離はみられない。 (5) 指針第七条第二号ニに関する調査項番1552及び、1553に係る適合例についてケーブルが防火区画を「貫通すること」「換気・冷房ダクトダンパ措置」を防火区画図面に基づき調査しているが、現在、防火区画として提出される書類が事業者提出の図面で確認しており、実際の防火区画を示しているかは判断できずその図面から読み取るしかない。 【電子署名法関連部分】 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十四条第二号イ 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四条第一号イ　等
10	認定認証業務で発行する利用者の電子証明書の記録項目の要件について、施行規則、指針に規定しているが、記録対象とその表示箇所等の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 施行規則第六条第五号に規定する電子証明書に表示する必須の記録事項の追加及びその表示する箇所を指定することの是非、例えばsubjectフィールドに入るべき電子証明書のプロファイルの特定等。また利用者の氏名等をsubjectフィールドにローマ字で記録する場合の利用者氏名の読みの確認方法について。 (2) 施行規則第六条第四号に規定する電子証明書の有効期間が5年を超えないものであることと、適合例項番3402の可否判断日から5年未満であることの表現の不一致について

	【検討内容】 (1) 多くの他業務をもち、また海外に多くの拠点を持つ認証事業者が、各事業者独自の仕様で海外において実績を上げているため、日本独自に仕様をかためることに抵抗感を持っており、法的な根拠のない制約（適合例といえども）を容認することが難しいことなどから、電子証明書のプロファイルを定義することはしていない。また、表記については各認定認証業務で規定を作成し、その規定に則り運用している。 (2) 電子証明書の有効期間の設定は、施行規則第六条第四号の適合例項番 3402 により、利用者に発行する電子証明書の有効期間は発行の可否判断日から起算して 5 年未満であるとしている。「証明の可否判断日」とは、利用申込が行われ真偽確認等審査の後、認証事業者が電子証明書の発行を承認した日のこと。従って「証明の可否判断日」+「電子証明書記載の有効期間」が 5 年未満であることが求められる。各認定認証業務ともこの要件が守られている。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第四号 電子署名及び認証業務に関する法律施行規則第六条第五号　等
11	認定認証業務で利用者署名符号を生成する場合、生成を行った後、安全・確実に利用者に送付することについて、施行規則に規定しているが、利用者署名符号の活性化に使用する PIN 等の生成から送付するまでに当該認証業務内での扱いについて、より明確化するための課題整理を以下のように実施した。 【課題整理のポイント】 (1) 利用者署名符号の生成指示に係る安全性についてどの段階から確認する必要があるか、安全性、確実性についての具体的な要件を検討する。 (2) 利用者署名符号を安全な状態に保つための保護方法（PIN の扱い）及び渡す方法についての具体的な要件を検討する。 (3) 本人限定受取郵便を使用する送達方法による利用者署名符号の送付と受領書の関係について整理する。 (4) 認定認証事業者が作成した利用者署名符号を、どのように電子的に安全・確実に利用者に送付することが可能であるかについて、検討する。 【検討内容】 (1) 利用者署名符号の生成指示に係る安全性について ・利用者署名符号の生成を指示するための要求データの作成段階から、利用者署名符号生成設備に、生成要求を送信するまでの工程を確認している。 ・利用者署名符号の安全性、確実性を担保する保護（盗聴（秘匿性)、改変防止（完全性)）についての措置を、施行規則第六条第三号の適合例項番 3302 と 3303 に基づき確認している。 (2) 利用者署名符号を安全な状態に保つための保護方法（PIN の扱い）及び渡す方法について ・PIN の生成状態を、施行規則第六条第三号の適合例項番 3304 に基づき確認している。 ・PIN の保護の方法について、施行規則第六条第三号の適合例項番 3304 に基づき確認している。 ・PIN の送付の仕方により、利用者署名符号の安全性への影響を、施行規則第六条第三号の適合例項番 3305 に基づき確認している。 (3) 本人限定受取郵便を使用する送達方法による利用者署名符号の送付と受領書の関係に

	ついて ・利用者署名符号の送付に関しては、施行規則第六条第三号に規定する安全かつ確実に利用者に渡すことができる方法に該当する本人限定受取郵便（基本型）で送付することが可能である。しかし、その利用者署名符号を活性化する PIN の送付を書留等の配達した記録が追える方法を使い利用者本人に送付する場合（但しダウンロード方式については、ダウンロード PIN を本人限定受取郵便で送付することが必要となる）は、利用者署名符号を本人限定受取郵便（特例型）で送付することを認めている。また、代人又は代理人に利用者署名符号を送付する場合も、PIN は、前述した方法と同様に別送扱いとしている。 ・受理期限の最大は、現在の認定認証業務では利用者署名符号を送付してから 45 日となっている。受理期限は、認定基準の要件にはないが、利用者署名符号を安全且つ確実に利用者に交付する（施行規則第六条第三号）ための合理的な期間の目安として 30 日を越える場合は、その根拠を確認している。現行、最長でも 45 日を越えないように指導している。 (4)利用者署名符号の受理を確認する期限の要件 ・全認定認証業務の利用者署名符号受理の期間の調査 ①株式会社日本電子公証機構認証サービス iPROVE ／受領書なし ②CECSIGN 認証サービス／受領書なし ③セコムパスポート for G-ID ／30 日 ④AOSign サービス／ 40 日 ⑤TOiNX 電子入札対応認証サービス／ 30 日 ⑥TDB 電子認証サービス TypeA ／45 日 ⑦ビジネス認証サービスタイプ 1／30 日 ⑧電子入札ｺｱｼｽﾃﾑ用電子認証サービス（ｼﾞｬﾊﾟﾝﾈｯﾄ株式会社） ／30 日 ⑨全国社会保険労務士会連合会認証サービス／ 30 日 ⑩CTI 電子入札・申請届出対応　電子認証サービス／ 35 日 ⑪税理士証明書発行サービス／ 30 日 ⑫日本司法書士会連合会認証サービス／ 30 日 ⑬e-Probatio PS2 サービス／ 15 営業日 ⑭日本土地家屋調査士会連合会認証サービス／ 30 日 ⑮MJS 電子証明書サービス／ 45 日 ⑯NTT ドコモ電子証明書サービス ／受領書なし ・受理期限の最大は現在利用者署名符号を送付してから 45 日となっている。受理期限は、認定基準の要件にはないが、利用者署名符号を安全且つ確実に利用者に交付する（施行規則第六条第三号）ための合理的な期間を設定することが出来き、目安として 30 日を越える場合は、その根拠を確認している。現行、最長 45 日を越える受理期限は 45 日を越えないように指導している。 (5)利用者署名符号を電子的に安全・確実に利用者に送付することが可能である提供方法 ①AccreditedSign ﾊﾟﾌﾞﾘｯｸｻｰﾋﾞｽ 2:Web インタフェースにより、RA 局に設置された PKCS#12 ダウンローダを経由し、IA 局に設置された RA/IA サーバからダウンロード（業務廃止により、現在は実施されていない） ②ビジネス認証サービスタイプ 1:Web インタフェースにより、RA 局に設置された PKCS#12 ダウンローダを経由し、IA 局に設置されたディレクトリサーバからダウンロード（業務廃止に向けて、電子証明書の発行を停止しており、現在は実施されていない） ③セコムパスポート for G-ID:利用者に公開されるダウンロードツールを利用者の環境にインストールし、当該インストーラからプログラムを実行することで、IA 局に設置された AP/DB サーバを経由し、IA 局に設置された CA サーバからダウンロード（2011 年 12 月の変更認定により、2012 年 1 月よりサービスを実施中） 実地調査により確認したダウンロード方式については、その提供方法の如何（Web インタフェース方式なのか、ダウンロードツール方式なのか）によらず、利用者へ提供される方

	法が堅持され、更新調査において当該方式についても確認し、認定調査（変更調査）において確認した方式から変更がないこと、もし変更があった際には事前に指定調査機関に問い合わせがあり、やむを得ざる事情が認められていることが条件であると思料する。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第三号 電子署名及び認証業務に関する法律施行規則第十二条第一項第一号リ 電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針 第４ ２．(1) 等
13	認定認証業務で発行する電子証明書の失効情報等の活用ならびに発行した失効情報(CRL等）の利用について、有効期間が終了した電子証明書の失効に関する署名検証者への対応方法については、適合例 3813 において実施方法を定めることが求められているが、失効情報の利用については、より具体的に活用や利用の基準を明確化するための課題整理を以下のように実施した。 【課題整理のポイント】 (1) 電子証明書の失効情報等の利活用に関する考え方についての CRL の再利用が、当該認定認証業務の一部として実施する形態となっていることについて (2) 発行した失効情報（CRL 等）の利用基準の明確化等についての DVCS 等での失効情報の蓄積、利用は認められる。なお、認定認証業務が DVCS 等に提供する場合は、この行為は、認証業務の範疇であると判断することについて、また VA については、一定の基準を設け、認定基準に盛り込むことの是非について 【検討内容】 (1) 失効情報等の利活用 電子署名法上、有効期間の切れた電子証明書の失効情報については、保存義務は明示されているものの、その利活用に関する規定はない。しかし、蓄積する CRL 内に、有効期間内の電子証明書の失効情報が含まれる場合、電子署名法の要件が係るので注意が必要である。CRL の再利用を、当該認定認証業務の一部として実施する場合には、変更の認定が必要である。 (2) 発行した失効情報（CRL 等）の利用基準の明確化 「有効期間が残存している証明書の失効情報は、認証局の発行している CRL を利用しなければならない。」としているが、一旦発行された CRL は、その利用について特別な制限を設ける必要はないものと考えられることから、DVCS 等での蓄積利用は、認められる。なお、認証局が DVCS 等に提供する場合は、この行為は、認証業務の範疇であると判断されるが、公開した CRL を取得し、これを利用する場合は、認証業務の範疇であると見做さないと考える。 【電子署名法関連部分】 具体的規定はないが以下の規定に関係する。 電子署名及び認証業務に関する法律施行規則第六条第十一号 電子署名及び認証業務に関する法律施行規則第十二条第一項第二号ニ 等
18	認定認証業務に係る帳簿書類について、設備関連の帳簿書類に係る保存要件（帳簿及び重要データを含む設備の廃棄、設備系帳簿保存期間の延長、帳簿廃棄記録の対象拡大、帳簿利用記録の内容等）の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 (1) 帳簿及び重要データを含む設備の廃棄 帳簿及び重要データを含む設備の廃棄について、完全に破棄または消去されることを要

	件として、認定認証業務を実施する事業者側での不用意な取り扱いによる漏洩等を未然に防ぐことについて (2) 設備系帳簿保存期間の延長 設備系帳簿保存期間の延長について、施行規則第十二条第三項では、作成した日から認定の更新の日までの保存義務が課せられる。しかし実地調査から認定の更新の日までの期間に作成された帳簿書類に関しては実地調査で確認することなく廃棄される可能性があるため、例えば作成した日から次々回の認定の更新の日まで保存する等の検討が必要 (3) 帳簿利用記録の内容 帳簿利用記録の内容について、「利用」の定義が不明確でなく記録することが難しいことから、「利用」の定義を明確化することについて 【検討内容】 (1) 帳簿及び重要データを含む設備の廃棄 帳簿を廃棄する場合、及び使用を終了する設備等に関し、それらに記録されている情報のうち重要な情報に関しては、外部の者に触れる前に完全に破棄または消去されることが望ましいが、そのことを要件として追加することにより、認定認証業務を実施する事業者側での不用意な取り扱いによる漏洩等を未然に防ぐことができると思われる。 (2) 設備系帳簿保存期間の延長 規則第十二条第三項では、第一項第四号に掲げる帳簿書類は、作成した日から認定の更新の日まで保存しなければならない。(参考；規則第十二条第一項第四号とは調査表 1000 番台)となっているが、この場合、前回の現地調査から認定の更新の日までの期間(1 ヶ月程度)の帳簿に関しては現地調査せずに廃棄されてしまう可能性がある。実際には、規則第十二条第三項の規定通り速やかに破棄している事業者はないので、当該期間中の帳簿内容は次の更新調査時に確認しているが、電子署名法での規定を望む。 その場合、現地調査以降に作成した帳簿としてしまうと、現地調査時までに事象が起こっていたとしても、現地調査時に帳簿化されていない場合もあるので、「作成した日から次々回の認定の更新の日まで保存」とした方が良いと思われる。 保存期間の過ぎた帳簿が廃棄されていたとしても電子署名法上の問題はない。しかし破棄されていた場合には、保存期間を少し延長してもらうよう事業者に相談することになると思われる。 (3) 帳簿利用記録の内容 帳簿の利用に関する記録は、規則第十二条第一項第四号トに規定されているが、「利用」の定義が明確でなく、記録することが難しいのが現状である。 「利用」とは、アーカイブ状態になったもの(例えば、サーバのログ等では、サーバに蓄積されたログを、DAT 等にバックアップしてアーカイブ保存したものを参照する場合は、利用とし、サーバに蓄積中のものを参照しても利用としない等。紙媒体の場合は、責任者の最終押印後のファイリングでアーカイブ状態とみなす等) 「利用」の定義が明確でなく、記録することが難しいのが現状である。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第十二条第一項第四号ト 電子署名及び認証業務に関する法律施行規則第十二条第三項　等
20	認定認証業務において利用者が利用者署名符号を他人に預けて管理することを前提に運用することについて、要件の明確化の課題整理を以下のように実施した。 【課題整理のポイント】 認定認証業務で発行する電子証明書は自然人に対して発行される。利用者が利用者署名符号を他人に預けて管理し、当該符号を使って電子署名を行うことが認められるのか。

	【検討内容】 利用者署名符号を他人に預けて管理することについて、「利用者署名符号については、十分な注意をもって管理する必要があること」が求められているが、その管理方法の要件及び、法制度上の利用者への制約は無い。したがって、認定認証業務においては、あらかじめ、利用者署名符号等の管理を e-文書拠点サーバにおいて行う運用方法を利用者に対して説明すればよいものと思われる。 【電子署名法関連部分】 電子署名及び認証業務に関する法律施行規則第六条第一号 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八条
21	認証業務が廃止される場合、廃止に係る手順、手続きが適切に実施されたことを確認する手段が無い。また、廃止後の帳簿書類及び発行者電子証明書等の管理方法が定められていない。 【課題整理のポイント】 (1) 認証業務廃止後の電子証明書の有効性確認について 認証業務が廃止される場合、現行規定では発行された電子証明書の有効性を確認できる電子証明書そのもの及び失効等情報の継続保存が規定されていないため、何らかの方法で、これらの情報が引き継がれることを検討する必要がある。 (2) 廃止後の関係書類及び発行者電子証明書等の管理方法について (3) 廃止過程又は廃止後の措置状況の確認について 【検討内容】 (1) 認証業務廃止後の電子証明書の有効性確認について 認証業務の廃止について、業務廃止時の CRL の発行手順は、事務取扱要領等に定められていることが要求されており、認定調査時に確認している。また、利用者からの失効請求等による CRL の発行手順も認定調査時に確認している。業務廃止時の CRL 発行操作は、利用者からの失効請求等による場合と同様であり、変更申請は不要である。 (2) 廃止後の関係書類及び発行者電子証明書等の管理方法について 廃止後の関係書類及び発行者電子証明書等の管理方法について、以下のように整理し、平成 23 年 2 月 23 日の実務者説明会にて、認定認証事業者に通知した。 ・適切な保存措置(漏えい、滅失又はき損防止措置) を施して保存すること。 ・1 年保存の帳簿書類については、保存は 1 年でよく、廃棄時に廃棄の記録を残すこと。 ・10 年保存の要件が課せられているもの(申込書類、規程類等)については、業務廃止後も施行規則第十二条第二項に基づき、引き続き保存すること。 ・利用者電子証明書、自己署名証明書、リンク証明書、相互認証証明書及び CRL/ARL 等を、電子データで保存する場合は、CD、DVD あるいは、DAT 等長期保存が可能で、読み出しに特別なソフトウェアを必要としないと思われる媒体で保存すること。 (3) 廃止過程又は廃止後の措置状況の確認について 廃止過程又は廃止後の措置状況を確認することについては、今後の検討が必要である。 【電子署名法関連部分】 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十二条第二項
22	戦争、テロ、天変地異、指定調査機関の調査員及び関係者が感染症に罹患、認証事業者の拠点が封鎖された等の不測の事態が発生することにより、調査業務継続ができない、若しくは、遅延する等の事態が発生し、認定更新調査及び変更調査等における調査が、認定

	期限あるいは、外部の要求等に伴い調査業務に事実上の調査期限が設定されている期限内に完了できない場合等の対応方法についての課題整理を以下のように実施した。 【課題整理のポイント】 (1) 期限までに完了できない場合の状況の整理 (2) 期限までに完了が必要な指定調査機関の調査具体例 (3) 対処方法案 (4) 調査を停止および再開する際の条件 (5) 延長の対象外となる事例の検討 【検討内容】 (1) 期限までに完了できない場合の状況の整理 ・申請受付が実施できないことによる ・実地調査が実施できないことによる ・報告書作成作業が実施できないことによる ・主務三省への事前説明が実施できないことによる ・正式通知が実施できないことによる ・事前説明時に不適合とした場合における以後の改善指導の実施ができないことによる (2) 期限までに完了が必要な指定調査機関の調査具体例 ・一般的な調査 ①認定更新調査 ②発行者署名符号の更新に係る変更調査 ・その他の調査 ①認証業務室等の移転等外部要因により調査期限が設定される調査 ②新たな利用者の電子証明書を発行停止として調査を行う変更認定に係る調査 以上のことにより、認定期限までに認定の更新や制限がある変更認定が行われない場合における法適合状態についての検討する必要がある。 (3) 対処方法案 ・指定調査業務が再開されるまでの間、緊急避難的に認定期限を延長する。 ・指定調査業務が再開後に調査をただちに実施し、調査の結果が「適合」であれば、それまでの期間を遡及適合状態と見なす。 (4) 調査を停止および再開する際の条件 指定調査機関は調査の停止および再開を主務三省と協議し、その承認に基づきただちに調査業務を停止すると同時に省令第十条に基づく申請書の提出を行う。 協議の開始の時期は指定調査機関である JIPDEC の会長が調査業務継続についての事実を認知した日とする。事業者に対してはその承認により、署名法第二十四条の義務における「正当な理由」として指定調査機関の義務を免れる。 (5) 延長の対象外となる事例の検討 ・事業者側に認定期限内に責めに帰すべき過失から生じた障害等が露見した場合についても、不測の事態等を理由に延長を認める必要があるかという検討が必要となる。 【電子署名法関連部分】 電子署名及び認証業務に関する法律 （認定の更新） 第七条 第四条第一項の認定は、一年を下らない政令で定める期間ごとにその更新を受けなけれ

	ば、その期間の経過によって、その効力を失う。 （調査の義務） 第二十四条 　指定調査機関は、調査を行うべきことを求められたときは、正当な理由がある場合を除き、遅滞なく、調査を行わなければならない。 （業務の休廃止） 第二十八条 　指定調査機関は、主務大臣の許可を受けなければ、調査の業務の全部又は一部を休止し、又は廃止してはならない。 　２　主務大臣は、前項の許可をしたときは、その旨を公示しなければならない。
23	認証設備室のパーテションの上部に設けられている格子状の開口部の措置状況について、規則第六条第十五号へに基づく「第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置」の観点から検討し、措置状況について整理した。 【課題整理のポイント】 (1) 指針第七条第二号ロの観点からの整理 (2) 規則第六条第十五号への観点からの整理 (3) 事例について 【検討内容】 (1) 指針第七条第二号ロの観点からの整理 　指針第七条第二号ロにより、認証設備室に関しては、「隔壁により区画されていること」が要件となっており、それに基づく適合例として以下の 2 つが記載されている。 ・認証設備室は、容易に破壊されない構造・強度を持った間仕切り壁又は隔壁により認証設備室以外の室と区分されている。（調査表項番 1531） ・認証設備室は、侵入が可能となるような開口部を設けていない。（調査表項番 1532） これらの適合例について整理した結果、認証設備室のパーテションの上部に格子状の開口部が存在しても、容易に破壊されない構造・強度を持ち格子の間隔が狭く人の侵入が不可能であれば、この 2 つの適合例の要件を満たしていると思料する。 (2) 規則第六条第十五号への観点からの整理 　規則第六条第十五号へにより、「第十二条第一項各号に掲げる帳簿書類の記載内容の漏えい、滅失又はき損の防止のために必要な措置」を講じることが要件となっており、それに基づく適合例として調査表項番 3C56 に以下が記載されている。 ① 共通要件 ・各記録は、施錠可能な出入口を持ち、間仕切り又は壁等によって区分された室の中に保存する。 ・各記録が保存される室には、自動火災報知器及び消火装置が備えられている。 ・各記録は直射日光が直接当たらない場所に保存するか、直射日光が当たらないよう、遮蔽措置を講ずる。 ② 紙媒体により原本で保存される資料等における追加要件 ・原本上の記録が判読不能とならない環境を備えている。 ・専用のファイルにとじ込む。 ③ 電磁的記録で保存される記録における追加要件 ・当該記録媒体の内容を表示することが出来るように、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを維持・保存しておくこと。特に、電子計算機その他の機器、オペレーティングシステム及びアプリケーションを更新する場合は、当該記録媒体との互換性を確保すること等により、表示不能を生じさせないこと。

	・記録媒体は、データの表示不能にならないように適切なケース等に保管する。さらに記憶媒体の特徴に合わせて適宜記録し直すなどの措置が実施されるようになっている。ただし、その際、保存内容の完全性・機密性を損なわない方法でなされている。 これらの適合例では、帳簿記載内容の漏えいに繋がる手段を個々に具体的に例示してはいないが、盗聴・盗撮等に関する技術的な進歩や、これらを可能にする機器の普及状況等を鑑みて、漏えい防止のために必要な措置状況を確認する必要があると思料する。 認証設備室のパーテションの上部に格子状の開口部が存在した場合、最近のデジタルカメラ、録音機能付携帯電話やスマートフォンの技術的な進歩及びその普及により、人間の侵入が不可能な開口部からデジタルカメラ等で盗撮することや、会話内容を盗聴することが可能な状況になりつつあり、適合例等には明示的に記載されてはいないものの、盗撮・盗聴による漏えいを防止する新たな対応が必要と考えている。 (3) 事例について 認証設備室のパーテションの上部に格子状の開口部があるケースは、以下の３事業者についてである。 ① 事業者１と事業者２に関しては、共通の IA 局を使用している。当該 IA 局の調査に関しては、新規の認定から平成 20 年 2 月の鍵更新の変更調査までを JQA（指定調査機関として、平成 20 年 2 月 29 日まで活動）が実施しており、平成 20 年 3 月の更新調査以降は JIPDEC が実施している。平成 19 年 8 月に認証設備室を現在の場所へ移転する変更調査が JQA によって実施され、適合との報告がなされている。この際に、認証設備室に関しては、パーティションの上部を 40cm ほど格子にして、煙の通り道を確保することにより、認証設備室内に新たな火災報知機を設置せずに消防法に適合させる措置がなされている。本件に関しては、過去に適合との判断に基づき認定を取得済みの事案であり、また、適合例等に明示的に想定されていないため、「指摘事項」として事業者に対応をお願いすることが難しい案件ではあるが、新たに発生した脅威に対処する必要があることを事業者にご理解いただき、今後の対応を実施していただけるよう、協議を継続中である。 ② 事業者３の調査に関しては、新規の認定から JIPDEC で実施している。認証設備室のパーテション上部を 50cm ほど格子にして 1.と同様の措置がなされている。当該事業者では、平成 24 年度中に認証設備室の移転が予定されており、その際に、パーテションの上部に開口部を設けないことを、事前のお問合せの際に確認している。 【電子署名法関連部分】 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七条第二号ロ 調査表項番 1531 調査表項番 1532 電子署名及び認証業務に関する法律施行規則規則第六条第十五号ヘ 調査表項番 3C55 調査表項番 3C56

3.1.2 (2) 暗号アルゴリズムの移行等に関する調査研究支援

平成23年度企業･個人の情報セキュリティ対策促進事業(電子署名･認証業務利用促進事業(暗号アルゴリズムの移行等に関する調査研究)) で開催された「電子署名法研究会」および作業部会（本人確認 WG）へのオブザーバー参加した。また研究会等の資料作成（暗号危殆化時の緊急時対応計画案の作成及びモデル案の作成等）および配付資料の事前確認作業を実施した。

電子署名法研究会は、下記のとおり実施され、オブザーバー参加および緊急時対応計画案の説明等をおこなった。

電子署名法研究会第 1 回　2011 年 10 月 28 日
電子署名法研究会第 2 回　2012 年 2 月 3 日
電子署名法研究会第 3 回　2012 年 2 月 22 日
本人確認 WG 第 1 回　2011 年 11 月 24 日
本人確認 WG 第 2 回　2012 年 2 月 1 日

この他、NISC からの依頼により暗号移行方針に基づく移行対応状況調査を暗号移行を検討している認定認証事業者に依頼し、回答をとりまとめ、経済産業省経由で回答を送付した。その結果、NISC から関係者に対して、暗号移行指針に基づく各認証局の移行対応状況調査に係る担当者意見交換会の開催案内があり、認定認証事業者へのご案内および 2012 年 2 月 23 日に開催された意見交換会に参加した。

1）暗号危殆化時の緊急時対応計画案

【雛型】

－電子署名法における暗号アルゴリズム移行研究会－

暗号危殆化時の緊急時対応計画

雛型

平成２３年３月

■本書の位置づけ

本書は、認定認証事業者が「暗号化危殆化時の緊急時対応計画」を定める場合の雛型である。

■本書を作成するにあたっての方針

他の規程を引用できる箇所は出来るだけ引用を用い、記述は出来るだけ簡潔にすること。

■本書の利用方法

・表紙の網掛け部分は、変更が必要な箇所を示している。
・本文中の網掛け部分は、適切に記述できることを目的としたコメントであるので、記述した後は削除すること。
・他の規程を引用する場合は、引用する規程の名称と引用する箇所を「」で囲んで記述すること。

■必須項目と任意項目

章節項	必須/任意	補足
1．基本方針	－	
1．1 目的	－	
1．2 対応フロー	－	
1．3 緊急時の例外対応	－	
2．体制	－	
2．1 実施体制	必須	
2．2 責任と権限	必須	
2．3 連絡先	必須	
3．条件	任意	パターン分けを行う場合に記述
4．現行アルゴリズムでの対応手順	－	
4．1 発行停止	必須	
4．2 利用者への通知	必須	
4．2．1 利用者への通知方法	必須	
4．2．2 利用者への通知内容	必須	
4．3 検証者への通知	－	
4．3．1 検証者への通知方法	必須	
4．3．2 検証者への通知内容	必須	
4．4 失効	必須	
4．5 CRL/ARL の公開	必須	

4．6 発行者署名符号の廃棄	任意	
4．7 主務省への報告	－	
5．新暗号アルゴリズムによる回復手順の決定方法	－	5章を記述する場合は、6章の記述は不要
5．1 回復手順の決定体制	（必須）	
5．2 回復手順の決定手順	（必須）	
5．3 主務省への報告	－	
6．新暗号アルゴリズムによる回復手順	－	6章を記述する場合は、5章の記述は不要
6．1 新暗号アルゴリズムへの移行	－	
6．1．1 検証環境の確認	（必須）	
6．1．2 移行手順	（必須）	
6．1．3 主務省への報告	－	
6．2 再発行	－	
6．2．1 利用者への通知方法	（必須）	
6．2．2 利用者への通知内容	（必須）	
6．2．3 再発行手順	（必須）	
6．2．4 主務省への報告	－	
7．計画の改定	－	
7．1 計画の改定手続き	必須	
7．2 計画の改定の通知	必須	
8．その他	任意	

注： 必須/任意欄の“－”は、記述済みであることを示す。

サービス名称

暗号危殆化時の緊急時対応計画

Version X.X

平成２×年××月××日

認定認証事業者名称

改訂履歴

Version	改訂内容	作成日/改訂日	作成者/改訂者	承認者
1.0	初版			

－ 目次 －

１．基本方針

１.１　目的

本書は、本サービスにおいて電子署名法の主務省から通知される暗号アルゴリズムの危殆化による緊急時に対応する対応計画を規定する。

主務省から緊急時対応計画の実施が発動された場合は、この規定を実施する。

１.２ 対応フロー

緊急時の対応フローを図 1-1 に示す。

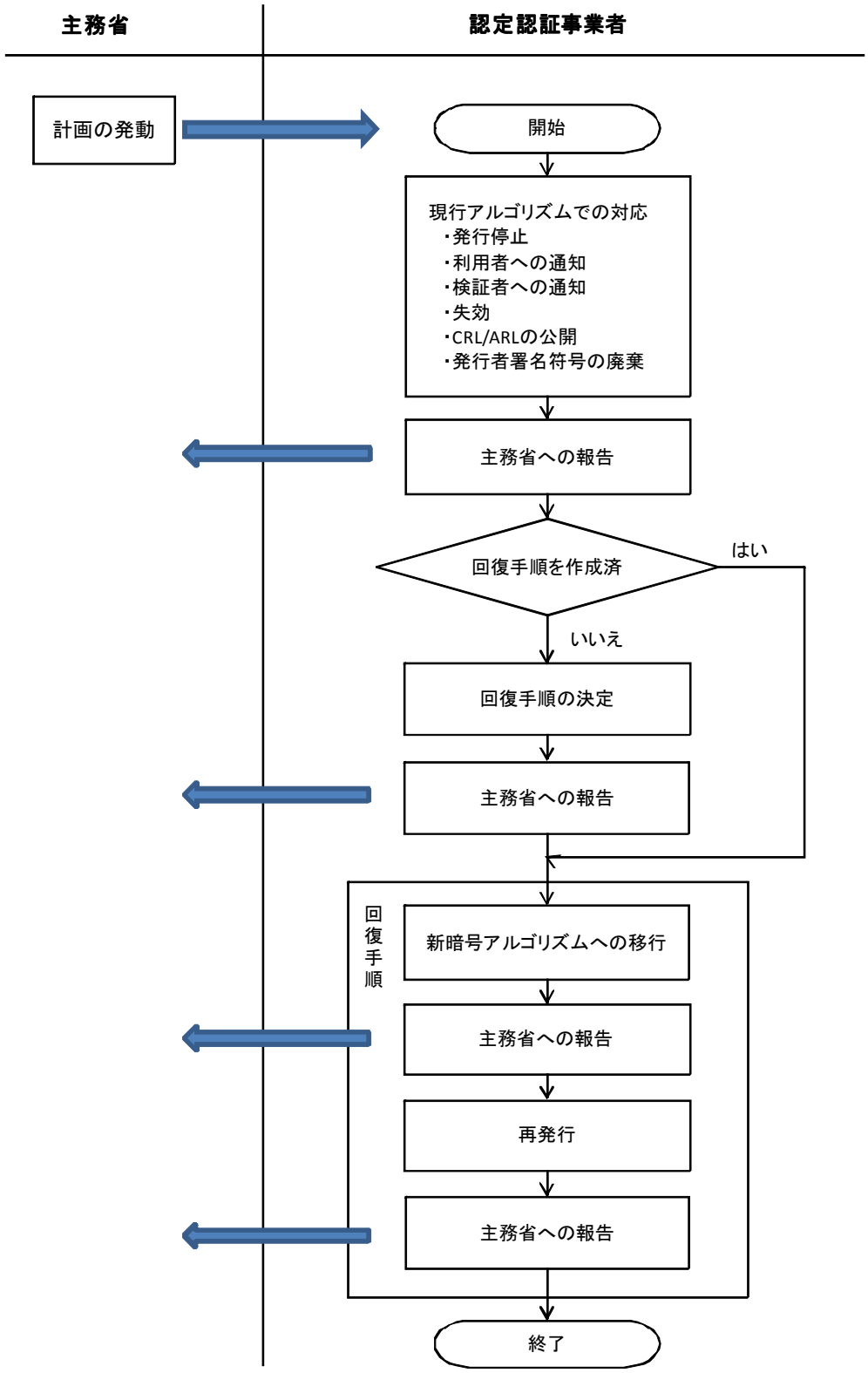

図 1-1 緊急時の対応フロー

１.３ 緊急時の例外対応

計画の実施時に、緊急時の例外対応として、責任者の判断により計画の内容以外の対処を行う場合がある。

例外対応を行った場合には、その内容と理由を速やかに主務省に報告する。

２. 体制

２.１ 実施体制

主務省から緊急時対応計画の実施が求められてから実施完了までの認証局の実施体制を図示する。

２.２ 責任と権限

実施体制の役割ごとの責任と権限を記述する。

２.３ 連絡先

緊急時に主務省から通知する連絡先として、担当者を２名記述する。

・連絡先１

所　　属：

氏　　名：

電話番号：

E メール：

・連絡先２

所　　属：

氏　　名：

電話番号：

E メール：

３. 条件

各項目を条件に分けて記述する際に、その条件をここで定義する。

条件は、【条件１】、【条件２】、…、【条件ｎ】と記述する。

（例）

【条件１】

新暗号アルゴリズム移行前の危殆化時の対応。

【条件２】

新暗号アルゴリズム移行後の危殆化時の対応。

4. 現行アルゴリズムでの対応手順

4.1 発行停止

通知を受けた後、認証局としてどのような手順で電子証明書の発行サービスを停止するのかを記述する。

4.2 利用者への通知

4.2.1 利用者への通知方法

利用者への通知をどのような方法で行うかを記述する。

4.2.2 利用者への通知内容

利用者への通知内容を記述する。
・危殆化した暗号アルゴリズムとその状況について
・現在有効な電子証明書の取扱について（失効させる/させない）
・新暗号アルゴリズムへの移行について（可能な場合）
・電子証明書の再発行について（可能な場合）
・その他

4.3 検証者への通知

4.3.1 検証者への通知方法

署名検証者への通知をどのような方法で行うかを記述する。

4.3.2 検証者への通知内容

署名検証者への通知内容を記述する。
・危殆化の内容（通知内容）
・その他

4.4 失効

有効な利用者電子証明書の全失効手順（またはそれに該当する処理手順）を記述する。

4.5 CRL/ARL の公開

失効させた電子証明書に対する CRL/ARL の発行手順および公開手順と時期について記述する。

4.6 発行者署名符号の廃棄

発行者署名符号の廃棄が必要な場合には、その手順について記述する。

4.7 主務省への報告

現行アルゴリズムへの対応がすべて完了したことを、様式第１を用いて主務省へ報告する。

5. 新暗号アルゴリズムによる回復手順の決定方法

新暗号アルゴリズムによる回復手順を計画には記述せず、発動後に決定する場合に、本章を記述する。

5.1 回復手順の決定体制

新暗号アルゴリズムによる回復手順を計画には記述せず、発動後に決定する場合に、回復手順を決定する体制を記述する。

5.2 回復手順の決定手順

新暗号アルゴリズムによる回復手順を計画には記述せず、発動後に決定する場合に、回復手順を決定する手順を記述する。

5.3 主務省への報告

新暗号アルゴリズムによる回復手順を決定したことを、様式第１を用いて主務省へ報告する。報告の際には、６章を記述した改訂版の緊急時対応計画を合わせて提出する。

6. 新暗号アルゴリズムによる回復手順

新暗号アルゴリズムによる回復手順を計画には記述せず、発動後に決定する場合は、本章の記述は不要であるため、各節・項には“未定”と記述する。

6.1 新暗号アルゴリズムへの移行

6.1.1 検証環境の確認

移行するために最小限確認しなければならない検証環境とその確認方法を記述する。

６.１.２ 移行手順

移行方法（新局方式/鍵更新方式、時期や対応期間によって変更するか否か等）や移行手順について記述する（条件があれば条件も記述）。

６.１.３ 主務省への報告

新暗号アルゴリズムへの移行をすべて完了したことを、様式第１を用いて主務省へ報告する。

６.２ 再発行

６.２.１ 利用者への通知方法

利用者への再発行の通知をどのような方法で行うかを記述する。

６.２.２ 利用者への通知内容

再発行する利用者への通知内容を記述する。
申請方法、有効期限、料金、開始時期、再発行手順等。

６.２.３ 再発行手順

再発行の方針（申請方法、有効期限、料金、開始時期及び終了予定時期等）と手順について記述する（条件があれば条件も記述）。

６.２.４ 主務省への報告

緊急時対応計画がすべて完了したことを、様式第１を用いて主務省へ報告する

７. 計画の改訂

７.１ 計画の改訂手続き

緊急時対応計画を改定する場合の手続きを記述する。

７.２ 計画の改定の通知

計画を改定した場合は、遅滞なく主務省に提出する。

８. その他

上記の構成の範囲外の内容だが、計画には記載しておかなければならないものを記述する。
節・項番については、上記を参考に追加すること。

様式第１

緊急時対応計画に基づく実施完了報告書

〇〇〇〇年〇〇月〇〇日

総　務　省
法　務　省
経済産業省

認定認証事業者名
認定認証業務名
認証局責任者　〇〇　〇〇 印

「暗号危殆化時の緊急時対応計画　Version X.X」に基づき、下記の作業が完了したことを報告します。

記

１．現行アルゴリズムでの対応手順

２．新暗号アルゴリズムによる回復手順の決定
新暗号アルゴリズムによる回復手順を記述した「暗号危殆化時の緊急時対応計画　Version X.X」」を添付します。

３．新暗号アルゴリズムへの移行

４．すべての作業の完了

備考　１．不要の文字は削除すること。
２．氏名を記載し、押印することに代えて、署名することができる。

【モデル案】

雛型を基にして、モデル案を作成した。

モデル案

○○認証サービス

暗号危殆化時の緊急時対応計画

Version 1.0

平成２×年××月××日

○○株式会社

Version	改訂内容	作成日/改訂日	作成者/改訂者	承認者
1.0	初版			

■本モデル案の位置づけ

平成 22 年度に開催された「電子署名法における暗号アルゴリズム移行研究会」において、認定認証事業者が暗号アルゴリズム（SHA-1 又は RSA1024）の危殆化に対する緊急時対応計画を策定する際の方針を次のように整理し、この方針を反映して「暗号危殆化時の緊急時対応計画 雛型」を作成した。

・計画は出来るだけシンプルにする
・他の規定を引用できる箇所は出来るだけ引用を用い、記述を少なくする
・計画は変更可能なように、改訂のプロセスを明記する
・回復手順（新暗号アルゴリズムへの移行、再発行）に関しては、発動後の回復手順の決定方法、決定後の主務省への報告内容を必須とし、回復手順自体の記述はオプション扱いとする
・計画の実施時、責任者の判断により、計画に盛り込まれた内容以外の対処を可能とする（ただし、事後に主務省へ報告を行う）

本モデル案は、認定認証事業者が「暗号危殆化時の緊急時対応計画 雛型」を基に、緊急時対応計画を策定する際の参考となるように、作成したものである。

（注）本モデル案では、「暗号危殆化時の緊急時対応計画 雛型」における誤字修正、表記の変更、4.2.1 と 4.2.2 の統合、及び 4.3.1 と 4.3.2 の統合を行っている。

■本モデル案の想定

・架空の認定認証事業者である
・通常の新暗号アルゴリズムへの移行は、新局立上げ方式ではなく、鍵更新方式を採用する
・回復手順（新暗号アルゴリズムへの移行、再発行）に関しては、回復手順の決定方法について規定することとし、回復手順自体については計画策定時には規定しない

－ 目次 －

１．基本方針

１.１　目的

本計画書は、本サービスにおいて電子署名法の主務省から暗号アルゴリズム(SHA-1 又は RSA1024)の危殆化による緊急時対応が発動された際に実施する内容を規定する。

１.２ 対応フロー

緊急時の対応フローを図 1-1 に示す。

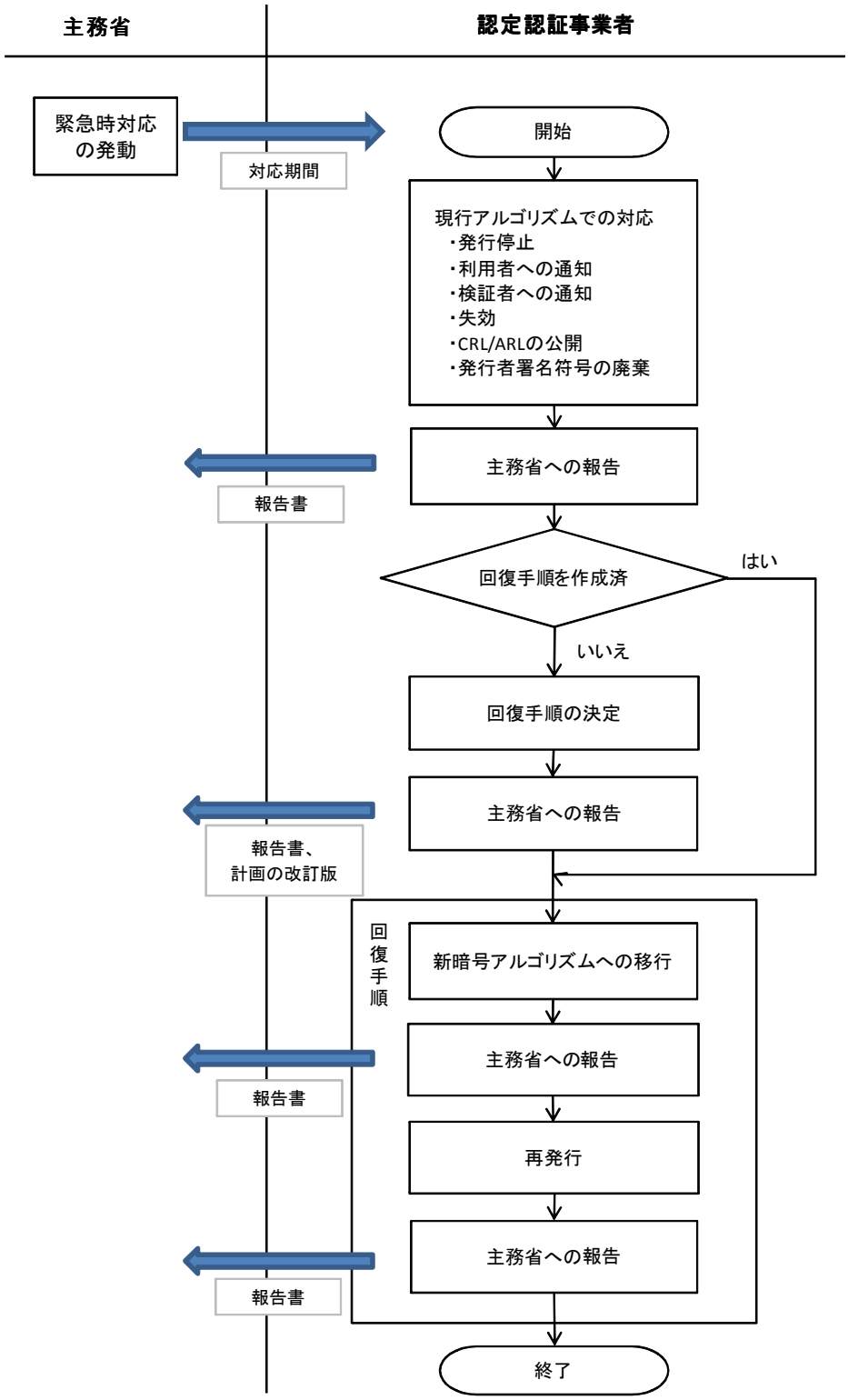

図 1-1 緊急時の対応フロー

１.３ 緊急時の例外対応

本計画の実施時に、緊急時の例外対応として、認証局責任者の判断により本計画書の内容以外の対処を行う場合がある。

例外対応を行った場合には作業記録を残し、例外対応の内容と理由とを速やかに主務省に報告する。

２. 体制

２.１ 実施体制

緊急時は、通常の実施体制の一部である図 2-1 の体制で実施する。

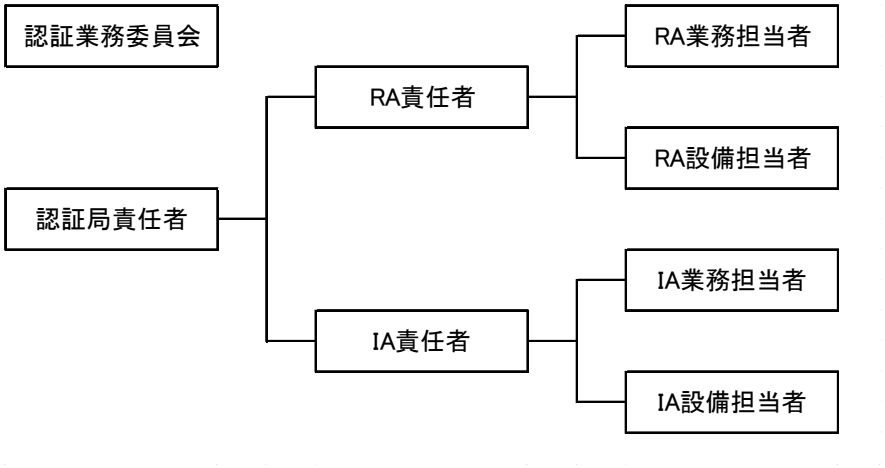

図 2-1　緊急時の実施体制

２.２ 責任と権限

(1)　認証業務委員会

本認証局の運営に係る意思決定を行う組織である。

認証業務委員会は、緊急時の対応に係わる事項の検討を行い、認証局責任者の決定を補佐する。また、本計画書の改訂が必要となったときは改訂内容の是非を検討し承認する。

(2)　認証局責任者

認証局における責任者である。本認証局を総括し、緊急時の対応が本計画書及びCPS等の規程に則って運用されることを管理する義務と責任を負う。緊急時の対応について、RA 責任者と IA 責任者へ作業指示を行い、その作業報告の確認を行う。

(3)　RA 責任者

登録局における責任者である。RA 業務担当者へ作業指示を行い、指示した作業が適切に実施されていることの監督と作業報告の確認を行って、認証局責任者へ報告する。また、RA 設備担当者の業務を承認し、登録局設備が適切な状態に維持されていることの監督と作業報告の確認を行って、認証局責任者へ報告する。

(4) RA 業務担当者

登録局業務における運用担当者である。RA 責任者からの作業指示に従い、作業を適切に実施する。作業後は RA 責任者に報告を行う。

(5) RA 設備担当者

登録局設備における担当者である。登録局設備を適切な状態に保つためのメンテナンス業務を行う。

(6) IA 責任者

発行局における責任者である。IA 業務担当者へ作業指示を行い、指示した作業が適切に実施されていることの監督と作業報告の確認を行って、認証局責任者へ報告する。また、IA 設備担当者の業務を承認し、発行局設備が適切な状態に維持されていることの監督と作業報告の確認を行って、認証局責任者へ報告する。

(7) IA 業務担当者

発行局業務における運用担当者である。IA 責任者からの作業指示に従い、作業を適切に実施する。作業後は IA 責任者に報告を行う。

(8) IA 設備担当者

発行局設備における担当者である。発行局設備を適切な状態に保つためのメンテナンス業務を行う。

2.3 連絡先

緊急時に係る連絡先は、次のとおりである。

・連絡先１

所　　属：　○○○○
氏　　名：　△△△△
電話番号：　XX-XXXX-XXXX
E メール：　aaaaaa@zzzz.co.jp

・連絡先２

所　　属：　○○○○
氏　　名：　□□□□
電話番号：　XX-XXXX-XXXX
E メール：　bbbbbb@zzzz.co.jp

３．条件

緊急時の対応は、主務省から緊急時対応の発動が行われた時の状況により異なる場合がある。以下に対応が異なる場合の条件について示す。

【条件１】

鍵更新方式による新暗号アルゴリズムへの移行前に発動された場合の対応を、条件１として示す。

【条件２】

鍵更新方式により新暗号アルゴリズムへは移行済みであり、旧暗号アルゴリズムによる利用者電子証明書の発行はすでに停止しているが、旧暗号アルゴリズムによる有効な利用者電子証明書がまだ存在している際に発動された場合の対応を、条件２として示す。

以下の項番において、緊急時対応の発動時に対応が異なる場合は、どちらの条件下での対応であるかを【条件１】又は【条件２】を用いて示す。
なお、【条件１】及び【条件２】の記述が無い項番は、どちらの条件にも該当することを意味する。

４．現行暗号アルゴリズムでの対応手順

４.１ 発行停止

【条件１】

危殆化した暗号アルゴリズムによる利用者電子証明書の発行を、次の手順で停止する。

① 暗号アルゴリズムの危殆化により発行サービスを停止する旨を、CP/CPS に規定する。
② 暗号アルゴリズムの危殆化により発行サービスを停止する旨をリポジトリにて公開するとともに、改訂した CP/CPS も公開する。
③ 利用申込み受付済みの利用者（ただし、電子証明書の送付は未完）に対しては、暗号アルゴリズムの危殆化により発行サービスを停止する旨の書面と、利用申込書及び申込時の添付書類一式を簡易書留にて送付する。

【条件２】

危殆化した暗号アルゴリズムによる発行サービスはすでに停止しているので、発行停止に関する対応は不要である。

４.２ 利用者への通知

【条件１】

利用者への通知内容と通知方法は、表 4-1 のとおりである。

表 4-1 条件１での利用者への通知内容と通知方法

通知内容	通知方法				
	CP/CPS	リポジトリ	メール(*1)	簡易書留(*2)	特定記録郵便(*3)
①危殆化した暗号アルゴリズムとその状況について	○	○	○	○	○
②危殆化した暗号アルゴリズムによる利用者電子証明書の発行を停止したこと	○	○	○	○	
③危殆化した暗号アルゴリズムによる利用者電子証明書で現在有効なものを全件失効させる（させた）こと	○	○	○		○
④新暗号アルゴリズムへの移行後の発行の再開に関しては対応が決まりしだい公開すること		○	○	○	
⑤暗号アルゴリズムの危殆化によって失効させた利用者電子証明書の再発行に関しては対応が決まりしだい公開すること		○	○		○

(*1) 有効な電子証明書を所有する利用者を対象とする。

(*2) 利用申込み受付済みの利用者を対象とする。利用申込書と添付書類一式を同封するので簡易書留を用いる。

(*3) 利用者電子証明書を失効させた利用者を対象とする。失効通知書を同封するので特定記録郵便を用いる。

【条件２】

利用者への通知内容と通知方法は、表 4-2 のとおりである。

表 4-2 条件２での利用者への通知内容と通知方法

通知内容	通知方法			
	CP/CPS	リポジトリ	特定記録郵便(*1)	
①危殆化した暗号アルゴリズムとその状況について	○	○	○	
②危殆化した暗号アルゴリズムによる利用者電子証明書で現在有効なものを全件失効させる（させた）こと	○	○	○	
③暗号アルゴリズムの危殆化によって失効させた利用者電子証明書の再発行に関しては対応が決まりしだい公開すること		○	○	

(*1) 利用者電子証明書を失効させた利用者を対象とする。失効通知書を同封するので特定記録郵便を用いる。

４.３ 検証者への通知

検証者への通知内容と通知方法は、表 4-3 のとおりである。

表 4-3 検証者への通知内容と通知方法

通知内容	通知方法	
	リポジトリ	
①危殆化した暗号アルゴリズムとその状況について	○	
②危殆化した暗号アルゴリズムによる利用者電子証明書で現在有効なものを全件失効させる（させた）こと	○	

４.４ 失効

危殆化した暗号アルゴリズムによる利用者電子証明書で現在有効なものを、次の手順で全件失効する。

① 認証局責任者が認証業務委員会の了承を得たのち、RA 責任者と IA 責任者に対して全件失効の作業指示書を作成する。失効事由は「keyCompromise」とする。

② IA 責任者は、IA 業務担当者に指示し、認証設備室にて相互牽制の上で CA アプリケーションの全失効機能を用いて、有効な利用者電子証明書の失効を行い、CRL を更新する。

③ RA 責任者は、RA 業務担当者に指示し、更新した CRL により失効情報の確認を行う。

④ RA 責任者は、RA 業務担当者に指示し、失効対象の利用者に対して失効通知を行う。失効通知には、暗号アルゴリズムが危殆化したため失効させたこと、今後の対応についてはリポジトリを参照してほしいことを含める。

⑤ RA 責任者と IA 責任者はそれぞれ作業報告書を作成し、認証局責任者に報告する。

なお、全件失効の詳細な手順については「○○手順書」を参照する。

４.５ CRL/ARL の公開

失効させた利用者電子証明書に関する CRL は、内容の確認後直ちにリポジトリで公開する。

失効させた全ての利用者電子証明書の有効期間が満了するまで、リポジトリに公開する。

４.６ 発行者署名符号の廃棄

【条件１】

発行者署名符号の廃棄は、新暗号アルゴリズムへの移行手順の一環として行う。

なお、発行者署名符号の廃棄に関する詳細な手順については「○○手順書」を参照する。

【条件２】

旧発行者署名符号はすでに廃棄済みなので、廃棄に関する処置は不要である。

４.７ 主務省への報告

現行アルゴリズムへの対応がすべて完了したことを、様式第１を用いて主務省へ報告する。

５. 新暗号アルゴリズムによる回復手順の決定方法

本認証局では、主務省から緊急時対応が発動された後に、以下の回復手順の決定体制及び決定手順により、新暗号アルゴリズムによる回復手順を決定する。

５.１ 回復手順の決定体制

回復手順については、認証業務委員会で内容を検討して決定する。

５.２ 回復手順の決定手順

回復手順の決定は、次の手順で行う。

① 主務省から緊急時対応計画の実施が発動された場合、認証局責任者が直ちに認証業務委員会を開催する。

② 認証業務委員会にて、回復手順の具体的な内容について検討し、承認を得る。

５.３ 主務省への報告

新暗号アルゴリズムによる回復手順を決定したことを、様式第１を用いて主務省へ報告する。報告の際には、６章を記述した改訂版の緊急時対応計画を合わせて提出する。

６. 新暗号アルゴリズムによる回復手順

本認証局では、主務省から緊急時対応が発動された後に回復手順を決定するので、本章に関して現時点では“未定”である。

６.１ 新暗号アルゴリズムへの移行

６.１.１ 検証環境の確認

【条件１】

未定。

【条件２】

新暗号アルゴリズムには移行済みなので、検証環境の確認は不要である。

６.１.２ 移行手順

【条件１】

未定。

【条件２】

新暗号アルゴリズムには移行済みなので、移行手順は不要である。

６.１.３ 主務省への報告

新暗号アルゴリズムへの移行をすべて完了した際は、様式第１を用いて主務省へ報告する。

６.２ 再発行

６.２.１ 利用者への通知方法

未定。

６.２.２ 利用者への通知内容

未定。

６.２.３ 再発行手順

未定。

６.２.４ 主務省への報告

緊急時対応計画がすべて完了した際は、様式第１を用いて主務省へ報告する。

７. 計画の改訂

７.１ 計画の改訂手続き

緊急時対応計画の改訂については、認証業務委員会で改訂内容を検討し、了承を得た後に改訂する。

その実施記録として、「認証業務委員会議事録」を作成するとともに、改訂履歴として、改訂内容、改訂日、改訂者及び承認者の記録を残す。

７.２ 計画の改訂の通知

計画を改訂した場合は、遅滞なく主務省に提出する。

８. その他

なし。

様式第１

緊急時対応計画に基づく実施完了報告書

〇〇〇〇年〇〇月〇〇日

総　務　省
法　務　省
経済産業省

認定認証事業者名
認定認証業務名
認証局責任者　〇〇　〇〇 印

「暗号危殆化時の緊急時対応計画　Version X.X」に基づき、下記の作業が完了したことを報告します。

記

１．現行アルゴリズムでの対応手順

２．新暗号アルゴリズムによる回復手順の決定
新暗号アルゴリズムによる回復手順を記述した「暗号危殆化時の緊急時対応計画　Version X.X」」を添付します。

３．新暗号アルゴリズムへの移行

４．すべての作業の完了

備考　１．不要の文字は削除すること。
２．氏名を記載し、押印することに代えて、署名することができる。

3.1.3 (3) 認定認証事業者の暗号移行方針状況調査

平成 22 年度電子署名･認証業務利用促進事業（暗号アルゴリズムの移行等に関する調査研究）で実施された「電子署名法における暗号アルゴリズム移行研究会」内で平成 23 年 11 月末までに各認定認証業務が暗号移行方式（新局立上げあるいは鍵更新）を決定することとしており、それに向けて事前確認を 8 月末に行い、最終的な確認として 12 月中旬に暗号移行を実施する予定の事業者にアンケートを送付し、暗号移行方針を調査した。

１）事前確認

業務廃止を決定している事業者および暗号移行を実施しないとしている事業者をのぞいた 11 事業者に下記の確認表を送付し、暗号移行方針に関する調査を実施した。

調査内容： 暗号移行方針に関する方針決定状況等
調査期間： 2011 年 8 月 19 日～2011 年 8 月 31 日
調査対象： 認定認証事業者 11 社
調査項目： ･暗号移行方式(新局立上げ方式または鍵更新方式)の決定状況
･変更調査及び更新調査同時実施の可能性
･提示スケジュールにおける調査の可能性
･課題や問題点

（確認事項１）

緊急時対応ではなく、現在予定されている平成 25 年度（2013）に実施予定の暗号アルゴリズム移行方式として、貴業務として新局立上げ方式または鍵更新方式のどちらの方式を採用しようとしているか、またその採用理由について、現時点での考え方をお聞かせください。

（確認事項２）

「電子署名法における暗号アルゴリズム移行研究会」では、鍵更新方式に係る調査の効率化として、変更調査と更新調査とを同時に実施することにより、効率化が可能であることについてもご報告しました（※別紙１における 3.2.3 を参照）。鍵更新に関するすべての手順が認定時あるいは事前の変更調査により確認されている前提で、鍵更新の立会いのみを実施するケースに限定し、更新調査と同時に実施するものです。同時実施が認められた場合、貴業務における変更調査（鍵更新）と更新調査の同時実施の可能性についてお聞かせください。（別紙３）として、想定される事務手続きの流れを示しました。

なお、昨年度実施したアンケートにおいても、同時実施での対応を可能と回答いただいた業務も多く、技術面･運用面において基本的には実施可能であると考えています。また、変更調査（鍵更新）と更新調査とを同時に実施した場合であっても、調査手数料については、往復の交通運賃及び宿泊料を除き、これらの調査を個別に実施した場合と同額となります。

（確認事項３）

（別紙４）において、貴業務が鍵更新方式を採用した場合に、指定調査機関が想定している 2013 年度（平成 25 年度）の調査スケジュールを提示します。暗号アルゴリズム移行に伴う調査実施時期について、提示スケジュールに沿った調査の可能性や貴業務の検討状況について、お聞かせください。

（確認事項４）

（別紙３）に示したように、現在の法制度下では、鍵更新により新しい発行者署名符号（新鍵）を生成後も、旧発行者署名符号（旧鍵）による業務を維持、継続する必要があります。新鍵は、変更認定が下り、新しい発行者署名検証符号に係る電子証明書のフィンガープリントが官報公示されるまでは、使用できません。しかし採用される PKI アプリケーションの仕様によっては、そうした業務運用が非常に困難であったり、何らかの問題が発生して円滑な移行の障害となるケースが想定されます。

貴業務が採用している現行の PKI アプリケーション、あるいは暗号アルゴリズム移行に際して採用予定の PKI アプリケーションにおいて、このような問題は発生しないでしょうか？

もし何らかの課題や問題点がある場合、ヒアリングを実施することも想定しています。このような点がありましたら、開示可能な範囲で以下にご記入ください。

【アンケート調査結果】

（確認事項１）移行方針の決定状況

	方針の決定状況	該当事業者数
1	新局立上げ方式の採用を検討中	0
2	新局立上げ方式の採用を決定	0
3	鍵更新方式の採用を検討中	0
4	鍵更新方式の採用を決定	9
5	どちらの方式にするかも含め検討中	2
6	検討していない	0

	方針の決定スケジュール	該当事業者数
1	決定済み	9
2	2011 年 11 月までに決定予定	1
3	2012 年 3 月末日までに決定予定	0
4	2012 年 4 月以降	0
5	不明	1

（確認事項２）変更調査及び更新調査同時実施の可能性

	変更調査及び更新調査の同時実施の可能性	該当事業者数

1	可能	8
2	不可能	0
3	不明	3

(確認事項３)提示スケジュールにおける調査の可能性

	提示スケジュールにおける調査の可能性	該当事業者数
1	問題ない	8
2	問題あり	1
3	分からない	2

(確認事項４)課題や問題点

	課題や問題の発生可能性	該当事業者数
1	あり	3
2	なし	8
3	不明	0

2)方式確認

調査内容： 暗号移行方針に関する方針決定状況等
調査期間： 2011 年 12 月 14 日～2012 年１月 12 日
調査対象： 認定認証事業者 10 社
調査項目： ・移行方式の確定について
・貴業務に特徴的な電子証明書アプリケーション
・一括失効について
・ハッシュ関数（SHA-256）のアルゴリズムについて

(確認事項１) 移行方式の確定について

緊急時対応ではなく、現在予定されている暗号アルゴリズム移行方式として、貴業務として新局立上げ方式または鍵更新方式のどちらの方式を採用とされたか、現時点での確定内容をお聞かせください。

(確認事項２) 貴業務に特徴的な電子証明書アプリケーション

貴業務から発行された電子証明書は、どのような用途で使用されることが一番多いでしょうか？現在有効と思われる電子証明書の発行枚数、及び把握されている用途について、おおよその割合をお聞かせください。

（記載例：JACIC 利用 85%、IA 業務アプリケーション 10%、未把握 5%）

(確認事項３) 一括失効について

貴業務が採用している IA 業務アプリケーションでは、利用者電子証明書の失効に際し、一括失効機能を持っているでしょうか？

また対応できなかった場合、ARL を発行しただけでは対応できない利用者の割合は、確認事項２でお答えいただいた何割くらいでしょうか？

（確認事項４）ハッシュ関数（SHA-256）のアルゴリズムについて

貴業務が現在採用している暗号装置は、製品として SHA-256 以上のアルゴリズムに対応しているでしょうか？現行使用している暗号装置が採用された際は、製品としてハッシュ関数のサポートが SHA-1 のみにしか対応できていないケースがあります。

また対応できていない場合であって､暗号アルゴリズム移行に際しても現在の暗号装置を継続使用される場合、ハッシュ関数（SHA-256）のアルゴリズム対応については、何を基準として実施されるのでしょうか？指定調査機関は、何により SHA-2 対応いただいていることの根拠を実地調査で確認することができるでしょうか？

【アンケート調査結果】

（確認事項１）移行方式の確定について

	方針の決定状況	該当事業者数
1	新局立上げ方式の採用を検討中	1
2	鍵更新方式の採用を決定	8
3	どちらの方式にするかも含め検討中	1

（確認事項２）貴業務に特徴的な電子証明書アプリケーション

	JACIC 利用	該当事業者数
1	95％以上	6
2	90％以上 95％以下	2
3	0％	2

	電子申請･電子契約等	該当事業者数
1	５％	2
2	0.5％	2
3	0.01％	2

	自社のアプリケーション	該当事業者数
1	100％	2

（確認事項３）一括失効について

	一括失効機能	該当事業者数
1	一括失効機能がある	3
2	一括失効機能がない	7

(確認事項４)ハッシュ関数（SHA-256）のアルゴリズムについて

	ハッシュ関数（SHA-256）のアルゴリズムについて	該当事業者数
1	対応済	3
	対応していない	7
2	HW の更改が必要	2
3	SW の更改が必要	5

3.2 情報共有

(1) 特定認証業務インフォメーション発信

認定認証業務（全 18 業務、9 月に 1 業務および 11 月に 1 業務廃止）に対し、下記のとおり情報提供を実施した。

回数	発信日	内容
第 1 回	2011/4/5	人事異動に伴う調査員の退任およびアシスタントの変更について
第 2 回	2011/4/20	東日本大震災による認定認証業務への影響調査について
第 3 回	2011/6/6	東北地方太平洋沖地震に伴う電子証明書等の臨時取扱いについて(第 2 報)
第 4 回	2011/6/8	夏期一斉休暇について
第 5 回	2011/10/17	事務所移転（予定）について
第 6 回	2011/12/8	事務所移転について（ご連絡）
第 7 回	2012/1/6	実務者説明会の開催について（ご案内）
第 8 回	2012/2/8	暗号移行指針に基づく各認証局の対応状況調査
第 9 回	2012/2/10	実務者説明会の開催について（確定）
第 10 回	2012/2/17	暗号移行指針に基づく各認証局の移行対応状況調査に係る担当者意見交換会（開催案内）
第 11 回	2012/3/6	認定認証業務で用いる暗号アルゴリズムの移行について

(2) 実務者説明会

特定認証業務を運営する事業者が共有すべき事項について整理の上、以下の三つを柱に 2 月 22 日当協会第 1-3 会議室にて、「平成 23 年度（2012 年）実務者説明会」を実施した。全 16 認定認証業務関係者よりの参加は、合計 46 名。

1) 変更認定について

「変更認定の事例集」、「変更認定の事例集（補足説明）」と「変更認定に該当しなかった事例集」を取り上げ、変更認定についての考え方や、軽微な変更として扱った例等について

①変更認定の事例集（一覧）
②変更認定の事例集（補足説明）
②変更認定に該当しなかった事例集

内容については、付録の実務者説明会資料を参照。

2) 実運用上から見た業務遂行時の留意点

認証業務の円滑な実施および認定の更新等の調査時における認定認証事業者の負担軽

減のため、これまでの調査における検出事項の中から、業務管理者、セキュリティ管理者、業務運用者等を対象に特定認証業務に従事する際に日常的に留意すべき事項等

①氏名（日本人、外国人）のローマ字の確認について
　内容については、別冊の実務者説明会資料を参照。
②商業登記していない個人事業主の真偽確認について
　内容については、別冊の実務者説明会資料抜粋を参照。
③電子証明書に記載する住所のローマ字表記の規定化について
　内容については、別冊の実務者説明会資料を参照。
④帳簿文書の保存と廃棄について
　内容については、別冊の実務者説明会資料を参照。
⑤その他、現地調査時に指摘の多い事項
　内容については、別冊の実務者説明会資料を参照。

3) 激甚災害時の対応について
内容については、別冊の実務者説明会資料を参照。

4) 配布資料
実務者説明会資料(別冊１)を配布した。

5) 実務者説明会後の変更認定についての相談への影響
実務者説明会後に、実務者説明会で取り上げた「変更認定の事例集（一覧)」と「変更認定に該当しなかった事例集」等に関連すると思われる相談としては、以下のような相談があった。

・認証業務の廃止と認証業務設備室の廃止
・リポジトリ URL 移行
・激甚災害における対応

(3) Web コンテンツの運用

電子署名及び認証業務の普及に資する Web コンテンツを運用した。Web コンテンツは、平成 22 年度までの事業で作成したものを運用した。また、ホームページ上で公開しているコンテンツを改訂して、公開するなど、適宜、内容についての更新を行った。

1) Web コンテンツの見直し

①既存コンテンツの改訂

・法人名称の変更

平成24年4月1日に、財団法人日本情報処理開発協会から一般財団法人日本情報経済社会推進協会へ法人名称が変更になったため、コンテンツ（調査表の表紙を含む）を改訂した。

・認定に係る調査手数料（料金積算表）の適用について

平成 23 年 4 月 1 日以降に受け付ける調査申請より改定された「調査手数料（料金積算表)」を適用することをホームページに公開した。

・住所および連絡先の変更

12 月 26 日（月）に事務所の移転があり、連絡先となる問合せ窓口の電話番号を修正した。

Web からの問い合わせメール窓口として、電子署名・認証センターのホームページにこの委託業務の窓口であることが分かり易くなるように修正した。

・電子署名･認証業務普及セミナーの更新

平成 23 年 1 月 18 日に、平成 22 年度電子署名･認証業務普及セミナーのコンテンツを掲載した。

2) Web コンテンツのアクセス状況

①全体

・アクセス数

2003 年度から 2012 年 2 月末日現在のアクセス数(全体)を下表に示す。

表 3.1　アクセス数(全体)

				2003年度	2004年度	2005年度	2006年度	2007年度	2008年度	2009年度	2010年度	2011年度※
合計				60,549	84,158	151,982	220,394	238,369	373,863	503,328	457,715	516,172
	①指定調査機関			19,134	8,827	26,161	48,379	25,107	29,697	37,952	23,832	15,953
	利用促進	②ハンドブック関連	小計	7,715	14,329	12,007	10,234	18,042	13,630	21,119	21,384	8,988
			パーソナル編	3,516	3,882	3,463	3,833	－	－	－	－	－
			ビジネス編	4,199	10,447	8,544	6,401	－	－	－	－	－
			ハンドブック	－	－	－	－	8,107	5,636	4,887	2,646	1,676
			標準集(法令集)	－	－	－	－	9,935	7,994	9,341	9,312	3,910
			事例集Ⅰ	－	－	－	－	－	3,293	2,683	5,737	1,191
			事例集Ⅱ	－	－	－	－	－	－	4,208	3,689	2,211
		③セミナー関連	小計	10,701	44,764	71,682	87,546	83,530	160,519	201,467	213,462	276,240
			2003年度資料	－	16,827	23,305	22,988	21,020	17,393	24,106	29,316	31,452
			2004年度資料	－	－	16,818	22,931	18,140	12,235	18,355	26,391	27,197
			2005年度資料	－	－	－	12,937	11,007	10,100	10,461	6,260	7,736
			2006年度資料	－	－	－	－	13,623	13,873	13,889	12,586	9,558
			2007年度資料	－	－	－	－	727	70,370	55,075	48,690	80,554
			2008年度資料	－	－	－	－	－	7,359	44,382	44,280	69,130
			2009年度資料	－	－	－	－	－	－	3,603	27,815	30,436
			2010年度資料※	－	－	－	－	－	－	－	－	6,264
			その他	－	27,937	31,559	28,690	19,013	29,189	31,596	18,124	13,913
	④電子署名・認証について			－	2,330	16,105	32,376	55,114	84,060	124,986	128,974	129,553
	⑤小計			22,999	13,908	26,027	41,859	56,576	68,289	79,562	50,513	49,602
		トップページ		22,999	13,908	26,027	41,634	32,370	35,871	33,741	24,791	19,027
		最新情報、リンク集等		－	－	－	225	24,206	32,418	45,821	25,722	30,575
	⑥英語			－	－	－	－	－	17,668	38,242	19,550	35,836

※ただし2011年度分は、2012年2月末日現在
※2010年度資料については(財)日本情報処理開発協会 電子商取引推進センターの事業によって本Webコンテンツで公開したものである

2005年8月と2007年3月に、大きくデザイン改訂を実施している。
（2007年は委託の予算を使用し外注、Search Engine Optimizationを実現した）

・前年度伸び率

表 3.2　前年度伸び率

2004 年度	2005 年度	2006 年度	2007 年度	2008 年度	2009 年度	2010 年度	2011 年度
139%	181%	145%	108%	157%	119%	94%	123%

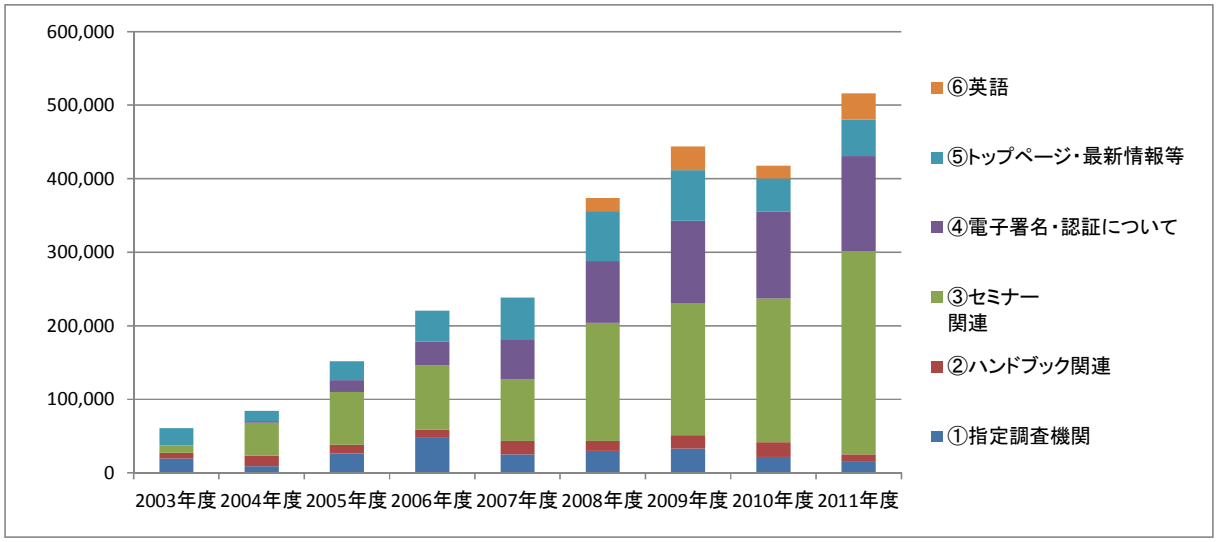
600,000
500,000
400,000
300,000
200,000
100,000
0
2003年度
2004年度
2005年度
2006年度
2007年度
2008年度
2009年度
2010年度
2011年度
⑥英語
⑤トップページ・最新情報等
④電子署名・認証について
③セミナー関連
②ハンドブック関連
①指定調査機関

図 3.1　アクセス数分類

②海外からのアクセス状況

アクセス数(全体)の内、外国からのアクセス状況を下表に示す。

表 3.3 海外からのアクセス状況

アクセス順位	2007年度		2006年度		2005年度		2004年度		2003年度	
1	.cn (中華人民共和国)	791	.ru (ロシア連邦)	672	.sg (シンガポール)	338	.tw (台湾)	57	.cc (ココス諸島(オーストラ	122
2	.nl (オランダ)	700	.ae (アラブ首長国連邦)	455	.th (タイ)	286	.edu (米国教育機関)	53	.nl (オランダ王国)	64
3	.ae (アラブ首長国連邦)	656	.cn (中華人民共和国)	242	.ru (ロシア連邦)	170	.nl (ニュージーランド)	31	.edu (米国教育機関)	56
4	.th (タイ)	571	.th (タイ)	224	.edu (米国教育機関)	116	.ro (ルーマニア)	19	.de (ドイツ)	49
5	.edu (米国教育機関)	359	.edu (米国教育機関)	204	.tw (台湾)	103	.de (ドイツ)	13	.tw (台湾)	35
6	.de (ドイツ)	251	.nl (ニュージーランド)	146	.de (ドイツ)	93	.uk (イギリス)	7	.au (オーストラリア)	33
7	.es (スペイン)	199	.no (ノルウェー)	139	.nl (ニュージーランド)	65	.ca (カナダ)	6	.fr (フランス)	21
8	.it (イタリア)	187	.br (ブラジル)	102	.my (マレーシア)	61	.ch (スイス)	5	.th (タイ)	10
9	.dk (デンマーク)	181	.de (ドイツ)	96	.at (オーストリア)	52	.th (タイ)	5	.ch (スイス)	8
10	.ca (カナダ)	147	.my (マレーシア)	88	.uk (イギリス)	46	.cn (中華人民共和国)	3	.no (ノルウェー)	8
11	.my (マレーシア)	144	.tw (台湾)	83	.fr (フランス)	43	.fr (フランス)	3	.tv (ツバル)	8
12	.no (ノルウェー)	122	.ws (サモア)	74	.za (南アフリカ)	40	.my (マレーシア)	3	.il (イスラエル)	7
13	.br (ブラジル)	119	.at (オーストリア)	47	.ro (ルーマニア)	32	.gh (ガーナ)	2	.ca (カナダ)	4
14	.mx (メキシコ)	107	.mk (マケドニア)	40	.gh (ガーナ)	30	.it (イタリア)	2	.sg (シンガポール)	4
15	.ar (アルゼンチン)	89	.it (イタリア)	32	.au (オーストラリア)	24	.mx (メキシコ)	2	.my (マレーシア)	3
16	.hu (ハンガリー)	86	.sg (シンガポール)	30	.ca (カナダ)	21	.sg (シンガポール)	2	.za (南アフリカ)	3
17	.tw (台湾)	83	.ci (コートジボワール)	20	.hu (ハンガリー)	20	.dk (デンマーク)	1	.uk (イギリス)	2
18	.do (ドミニカ共和国)	72	.se (スウェーデン)	20	.ch (スイス)	18	.es (スペイン)	1	.ar (アルゼンチン)	1
19	.pt (ポルトガル)	70	.uk (イギリス)	19	.hk (香港)	18	.il (イスラエル)	1	.at (オーストリア)	1
20	.kr (大韓民国)	66	.ua (ウクライナ)	16	.pl (ポーランド)	18	.in (インド)	1	.be (ベルギー王国)	1

アクセス順位	総計		2011年度 (2011年2月末まで)		2010年度		2009年度		2008年度	
1	.hu (ハンガリー)	20476	.hu (ハンガリー)	20319	.de (ドイツ)	2775	.nl (オランダ)	590	.cn (中華人民共和国)	753
2	.ru (ロシア連邦)	5693	.ru (ロシア連邦)	3265	.ru (ロシア連邦)	1174	.ru (ロシア連邦)	530	.nl (オランダ)	595
3	.de (ドイツ)	5354	.de (ドイツ)	1600	.in (インド)	788	.cn (中華人民共和国)	443	.de (ドイツ)	471
4	.cn (中華人民共和国)	3122	.cn (中華人民共和国)	583	.tz (タンザニア)	464	.tz (タンザニア)	411	.it (イタリア)	220
5	.nl (オランダ)	2384	.lv (ラトビア)	167	.cn (中華人民共和国)	363	.in (インド)	218	.ae (アラブ首長国連邦)	192
6	.th (タイ)	1427	.uk (イギリス)	157	.arpa (インターネットインフラ)	303	.it (イタリア)	203	.ca (カナダ)	155
7	.ae (アラブ首長国連邦)	1356	.au (オーストラリア)	156	.tw (台湾)	235	.edu (米国教育機関)	176	.es (スペイン)	135
8	.in (インド)	1179	.se (スウェーデン)	155	.ua (ウクライナ)	233	.tw (台湾)	162	.uk (イギリス)	117
9	.edu (米国教育機関)	1155	.il (イスラエル)	153	.se (スウェーデン)	222	.br (ブラジル)	161	.tw (台湾)	114
10	.tw (台湾)	938	.it (イタリア)	146	.pk (パキスタン)	218	.mm (ミャンマー)	151	.uk (イギリス)	117
11	.tz (タンザニア)	911	.ua (ウクライナ)	130	.nl (オランダ)	194	.de (ドイツ)	123	.fr (フランス)	105
12	.it (イタリア)	862	.th (タイ)	89	.th (タイ)	168	.ro (ルーマニア)	109	.in (インド)	116
13	.uk (イギリス)	542	.nl (オランダ)	86	.ci (コートジボアール)	166	.au (オーストラリア)	109	.dk (デンマーク)	115
14	.sg (シンガポール)	522	.lt (リトアニア)	81	[未知ドメイン名]	164	.to (トンガ)	94	.tw (台湾)	114
15	.au (オーストラリア)	487	.tw (台湾)	67	.lv (ラトビア)	109	.uk (イギリス)	90	.fr (フランス)	105
16	.ca (カナダ)	468	.in (インド)	66	.edu (米国教育機関)	109	.dk (デンマーク)	79	.int (国際機関)	100
17	.br (ブラジル)	460	.cz (チェコ)	55	.au (オーストラリア)	97	.ca (カナダ)	76	.arpa (インターネットインフラ	91
18	.se (スウェーデン)	429	.us (アメリカ合衆国)	52	.sg (シンガポール)	93	.lv (ラトビア)	56	.ro (ルーマニア)	87
19	.es (スペイン)	398	.eg (エジプト)	42	.fr (フランス)	75	.fr (フランス)	54	.pl (ポーランド)	77
20	.my (マレーシア)	386	.fr (フランス)	40	.mm (ミャンマー)	74	.cz (チェコ)	51	.ch (スイス)	76

3.3 ホームページのセキュリティ対策

Web コンテンツを公開しているサーバのセキュリティ対策を行うとともに、脆弱性検査を実施した。

1) セキュリティ対策

IPS（Intrusion Prevention System）及びファイアウォールによって防御されたセグメントに一般問い合わせ受付時のみ使用される受付 Web サーバを配置している。公開 Web サーバについては、年 1 回の電源の定期検査時に停止させないで済むように外部サイトに移す作業を実施した。

2) 脆弱性検査結果

Web コンテンツの公開 Web サーバ及び一般問い合わせ受付時のみ使用される受付 Web サーバについて、以下のとおり脆弱性検査を実施した。

(a) ネットワーク脆弱性検査

表 3.4 脆弱性検査結果

検査日	2012/3/ 7 ～13
対象ホスト	公開 Web サーバ、受付 Web サーバ
検査対象ポート	80（http）/443（https）
検査項目	インターネット経由のリモート検査により、以下が実施された。 ● ポートスキャン(TCP/UDP) ● バージョン調査 ● 起動サービスに対する脆弱性検査（動作に影響を与えない範囲） Web サーバ検査 メールサーバ検査 DNS サーバ検査など
検査結果	危険度 Medium の脆弱性を検出 OpenSSL の問題では、推奨されない暗号スイートの使用が検出されている。この脆弱性により、通信データの改ざんを検知することが困難となるため、使用しない事が推奨される。 脆弱性の対応については、３月 27 日に対応した。

(b) Web アプリケーション脆弱性検査

表 3.5 脆弱性検査(受付 Web サーバ)

検査日	2012/3/ 7 ～13
対象ホスト	受付 Web サーバ
検査対象ポート	80（http）/443（https）
検査項目	インターネット経由のリモート検査により、以下が実施された。 リクエストごとの検出対象脆弱性一覧 ● SQL Injection ● OS Command Injection ● Parameter Manipulation ● Cross-Site Scripting ● Insecure Cookie ● Error Code ● Buffer Overflow ● Session Fixation ● Cross-Site Request Frogery ● Insecure Protocol ● Unnecessary Informatio サイト全体における検出対象脆弱性一覧 ● Unnecessary File ● Misconfigured Server Setting ● Known Vulnerability
検査結果	危険度 Medium の脆弱性を検出 検出された脆弱性により、セッション ID が漏えいする可能性がある。 脆弱性の対応については、3 月 27 日に対応した。

4. 有識者への意見照会

4.1 一般問い合わせ Q&A

2.1 で整備した一般問い合わせ Q&A を外部有識者 3 名に送付し、以下のご意見を頂いた。

(諮問委員からのご意見)

a) 手塚委員

１．電子証明書

ご意見	
Q1	特に問題なし。
Q2	使用用途の例があるとより理解をますと思われる。
Q3	個人と自然人の用語が違うので、この関係を明確にする必要がある。
Q4	特に問題なし。
Q5	特に問題なし。
Q6	「電子証明書で署名する」の表現は良くなく、「電子証明書を使用して、署名する」の表現の方が良い。
Q7	特に問題なし。
ご意見	
Q1	特に問題なし。
Q2	認定認証業務一覧サイトの URL を加える方が良い。
Q3	特に問題なし。
３．電子署名について	
ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
Q5	特に問題なし。
Q6	「電子証明書で署名する」の表現は良くなく、「電子証明書を使用して、署名する」の表現の方が良い。

４．電子署名を使用したアプリケーションについて

ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
Q5	特に問題なし。

Q6	特に問題なし。
Q7	特に問題なし。
Q8	特に問題なし。
Q9	特に問題なし。
５．電子署名法の解説	
ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
６．電子署名･認証センターについて	
ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
Q5	特に問題なし。
Q6	特に問題なし。
Q7	特に問題なし。
Q8	特に問題なし。
7．全体に対して	
ご意見	
Q&A に関しては、全体的にうまく纏めていると思う。	

b)早貸委員

１．電子証明書

ご意見	
Q1	
Q2	
Q3	
Q4	「法人登記の情報を基に」→「商業法人登記の情報を基に」 「法務省登記所で発行される」→「法務省の電子認証登記所が電子証明書を発行する」 理由：用語の修正等（登記所の名称等は法務省が使っている用語に修正。「制度」が発行される訳ではないので、言いまわしの修正。
Q5	
Q6	

２．電子署名の概念や仕組みについて

ご意見	
Q1	
Q2	
Q3	第一段落：「署名には、・・2つの用語が用いられています」→　意図が分かりづらいです。そもそも設問の、「「電子署名」の用語解説として、電子署名とデジタル署名のどちらを用いたほうが良いでしょう」というのも意図が伝わりづらいと思います。設問と回答の第一段落を調整して、設問を、「電子文書に対する署名については、「電子署名」といわれたり、「デジタル署名」と言われたりしているようですが、どちらを用いたほうがよいでしょうか?」にしてはどうでしょう？ 第2段落：デジタル署名との対比としての「電子署名」一般に関する用語解説に電子署名認証業法中の定義を持ち出すのはミスリーディングだと思います。 第3段落：「広義の」電子署名は、作成者を示すためにされるものであるべきではありますが、作成者の特定や改変されていないことの確認ができなくても良いので、この記載は絞りすぎではないでしょうか？ 「広義の電子署名は、作成者を示すために行われる電子的な表現のこと全般を示すものとして使われる場合がありますが、このQ&Aにおいては、このうち、電子情報の作成者を特定し、署名を付した電子情報（データ）が改ざんされていないことを確認することができるもの（デジタル署名がその一例）を「電子署名」と呼ぶこととします。」と書くのでしょうか。（以降の回答でそのように用いられているので。） なお、電子署名認証業法による電子署名の定義は、これらの一般的な用語とは別に、電子署名認証業法を適用する上での特別な使いかたであることを整理した上で、記載すべきであると考えます。

３．電子署名について

	ご意見
Q1	1行目「発信主体」→「作成者」 「発信されたデータが」→「当該電子情報が」　※電子署名は電子情報の作成者を示すもので「発信」行為とは関係ありません。また、ひとつの文章中で、「電子情報」と「データ」が混ざると、同じものなのか、別のものなのかがわからなくなってしまいます。 1行目「本人」→　裸で「本人」といわれても・・・。作成名義人本人とか、何か必要であるように思います。 2行目「証明するために用いられます」　→　「電子署名とは、」で書き出しているので、「確認できるようにするために用いられる技術です。」　とか、でしょうか。　「証明」は訴訟法上の意味を持つ言葉ですし、電子署名は証明行為ではないので、書きぶりの精度に少し問題があるように思います。 4行目：「入札資格を持つ本人」　→　「本人」が裸です。上記に同じ。 5行目：「証明するために」→「確認できるようにするために」 「認定認証業務が発行する電子署名を使用して」→　電子署名一般の話から、電子署名認証業法で定義される電子署名の話になってしまっています。Q2以降は、電子署名法上の電子署名の話に限定されていないようなので、この設問において、電子署名法上の電子署名の効果や認定認証業務の話をするのであれば、第1段落の後に、電子署名認証業法3条の法的効果の説明をする段落を挿入した上で、電子入札では、認定認証業務により発行された電子証明書で検証可能な電子署名を付すことが求められる場合がありますとか、法的効果が後日問題となる可能性のある契約書等を電子的に作成する場合についても、認定認証業務により・・・・ことが推奨されます。」とかと続けるのがよいのではないでしょうか？ 「電子証明書を使用して電子署名する」　→　随所に「電子証明書を使用して電子署名する」「電子証明書で電子署名する」と言う記載がありますが、「電子証明書」は署名ツールとか鍵そのものではないはずなので、この表現は（少なくとも電子署名認証業法ととの関係では）正しくないと考えられます。
Q2	2行目：PiwerPointの後ろの閉じかっこ 3行目から4行目：「電子証明書で電子署名する」とは言わない（上記Q1記載のとおり） 5行目：「一般的に電子証明書を販売している認証局」→「一般的に電子入札用の電子証明書を販売している認証局」

Q3	少なくとも電子署名認証業法上の電子署名は、送信行為の一部として行うものではないので、設問については、「電子メールに電子署名を付して送信する方法について・・・」であるべきでは？ ①：「電子証明書で電子署名する」というロジックで書かれていますので、要修正 ②：インストールは、電子証明書だけではなく、鍵（鍵という言葉で良いかどうかは自信がないですが、１．の Q7 で登場しているので、大丈夫かと。）も必要 ③：「電子証明書で電子署名」がまた出てきています。 ④：「確認方法」　→　何の確認方法かを書くべき。
Q4	設問：「電子メールを読むために」でよいですか？ 注）　「パブリックとは」　→　「パブリック電子証明書とは」 　「証明書ストア」は説明なしで大丈夫でしょうか？
Q5	
Q6	設問では、電子印を押す＝電子署名する、となっているので、広義の電子署名の定義（上記）に従っているように見えますが、一方で、第 2 段落では、「電子署名」の語が電子署名認証業法の定義に係る電子署名を指している（原案は、推定効に触れるには要件が不足していて不十分と言う問題もありますが。）ので、意味不明になってしまっています。この設問で言いたかったことは何なのでしょう？

４．電子署名を使用したアプリケーションについて

ご意見	
Q1	
Q2	設問：「電子証明書」の導入でよいですか？　　そもそも「電子証明書」って導入するものかと言う点もありますが。
Q3	我が国の民法上は、契約の成立には、署名捺印等は不要です。意思が合致すれば契約は成立し、形式要件は求められません。この設問の回答は完全に誤り。 画像情報も広義の電子署名に含まれますし。 契約書等に署名押印をするのは、契約を成立させるためではなく、後日紛争になった場合の訴訟コスト（立証コスト）を抑えるためなので、誤解のないようにしてください。日本では、契約は口頭でも「成立」します。
Q4	
Q5	
Q6	会社設立等の登記のオンライン申請と、電子定款のオンライン認証の話が混ざってしまっているように見えます。会社の登記のオンライン申請と、電子定款のオンライン認証は、別の話だし、申請先も別（前者は登記所、後者は公証役場）。整理が必要です。どっちのことを書きたかったですか？、

Q7	Q6 と同様、登記のオンライン申請と、電子定款のオンライン認証の話が混ざっています。代理人として前提とされているのは、前者の場合は司法書士、後者の場合は、司法書士、行政書士。弁護士はどちらも。この設問は、登記申請と、定款認証にしっかり整理した上で、士業のみなさんの間の業際問題に巻き込まれないよに上手に書かなければなりません。要見直しですね。どちらのことが書きたかったでしょう？
Q8	
Q9	「電子契約書として取り結ぶ」とは言わないです。「契約書を電子的な手段で作成することは可能」とかでしょうか。 電子署名が必要かどうかも国によってことなるので、「契約書には契約を結び両者が電子署名することになります」と書くのは書きすぎ。 相手の国の法律を確認する前に、雇用契約に適用される準拠法がどの国の法律になるかを確認しなければなりません。この書き方だと相手国の法律の適用を前提としているように読めます。 雇用契約の場合は、通常の契約と異なり、労働法規制の影響を受けるので、電子契約一般の話を書くのか、雇用契約に絞った話を書くのかを決めなければなりません（それによって、準拠法ルールも変わってきます。） どう直せば良いのかは、もう少し何について記載したいのかを伺わないと判断できませんが、 １、雇用契約の契約書を電子的な方法で作成できるかどうかは、国によって異なる可能性がある（労働者保護に厚い国の場合などは、所定の様式等がある場合があり得る。） ２．可能かどうかは、その契約に適用される準拠法に依存する ３．雇用契約（労働契約）や消費者との契約については、一般的な契約とは異なる、準拠法決定ルールや契約成立のための要件が定められている場合が多い 等を前提に再考していただくと良いと思います。
５．電子署名法の解説	
ご意見	
Q1	
Q2	
Q3	
Q4	法律の条文を貼っているだけですが、一般向けの説明として足りますか？
６．電子署名･認証センターについて	
ご意見	
Q1	
Q2	
Q3	
Q4	
Q5	
Q6	

Q7	
Q8	

7．全体に対して

ご意見

b)宮内委員

１．電子証明書

ご意見	
Q1	（①～④と，⑤の字下げの位置が違います）
Q2	他の回答にくらべて，書き方が丁寧すぎるように思います（「異なっております」→「異なっています」，「お知りになりたい」→「知りたい」でいかがでしょうか）。
Q3	できれば，根拠条文を明記したいところです（法６条１項２号，規則５条 でしょうか？）
Q4	内容に特に問題はありません。ただし，最後の文の「……でも法人に」は「……で法人に」にした方がよいでしょう（商業登記認証局でも法人そのものに対する電子証明書を発行していると誤解される可能性があります）
Q5	
Q6	内容に問題はありませんが，Q に対する答えを最初に書くべきです。すなわち「電子文書に……課金されません。ただし，一般的には……費用が発生します。」とすべきです。

２．電子署名の概念や仕組みについて

ご意見	
Q1	
Q2	
Q3	第４段落の「電子署名とは，デジタル署名を……確認できます。」を最初の段落の次に記載すべきです。その上で，電子署名やデジタル署名の具体的な説明をするのがよいと思います。 (現状の)第２段落の最後の文が，法文のまま「推定する」で終わっているのはまずいので，「推定するものです」等に書き換えるとよいと思います。 最後の段落は，意味がわかりません。定義上，電子署名コデジタル署名 のはずなので，この段落の意味は，PKI を使っているがデジタル署名ではない，ということでしょうか？ そうだとしたら，事実に反しています。

３．電子署名について

ご意見	
Q1	「電子入札などでは」は「例えば電子入札では」としてはどうでしょうか。このままの文章だと，電子入札以外のアプリケーションでも入札書に署名を求められることがある，という意味になってしまいます。
Q2	内容に問題はありませんが，最初の文の「多くの場合」というのが少しわかりにくいので，冒頭を「多くの電子文書を作成する……」として，「多くの場合」を削除してはどうでしょうか。
Q3	最初の文が完結していないので，「送受信の手順を簡単に説明すると，以下のようになります」等の表現をとってはいかがでしょうか。
Q4	いきなり「パブリック電子証明書を利用する場合」と書かれてもわからないと思います(注があるにしても，唐突に感じます)。最初の柱書きに，パブリック電子証明書を利用するかどうかで手順が変わること，パブリック電子証明書とは何か(「注」に相当する内容)を書く方がよ

	いと思います。
Q5	2 文目の最初は「なお」ではなく「ただし」とすべきだと思います。
Q6	「法的に真正に成立したものと推定されます」はちょっと変です。そもそも，電子署名法を参照しているので，「法的に」は不要です（どうしても入れたいのなら，「……と法的に推定されます」でしょうか）。また，「真正に成立」と言われても，普通の人には意味がわからないと思うので，「（その電子文書が本人の意思により作成されたこと）」等の説明が要ると思います。

４．電子署名を使用したアプリケーションについて

ご意見	
Q1	「台九号」は「第九号」の誤植ですね。
Q2	
Q3	
Q4	
Q5	
Q6	
Q7	
Q8	記載の内容は間違っていないのですが，読みにくいです。 まず，「4.A4」記載のデ協のタイムスタンプはオンラインでないとできないことを記載し，その上で，あえてオフラインでやるとしたら……，という書き方をするのがよいと思います（デ協のタイムスタンプ局以外のものを使うのは，お勧めできませんよね）
Q9	国内であっても，労働条件の明示は書面による（労働基本法 15 条 1 項， 労働基準法施行規則 5 条 3 項）とされていますが，これは大丈夫なのでしょうか（電磁的記録でよいとは書かれていませんので，紙の文書が必要なのではないかと思うのです）

５．電子署名法の解説

ご意見	
Q1	説明の文章は，法文には忠実ですが，わかりにくいです。もう少し，一般の方にわかりやすい表現をとるべきだと思います。（Q1 は，認証業務を行おうとする人以外の一般人も読む可能性のある問いだと思います）
Q2	電子署名法の規定は条項を具体的に挙げるべきです。「……更新する必要があり（同法 7 条 1 項，同法施行令 1 条），」という具合です。
Q3	
Q4	ここでも，真正な成立の説明を入れたいところです（３．Q6 のコメント参照）

６．電子署名･認証センターについて

ご意見	
Q1	
Q2	

Q3	最初に，「可能です」と明言するほうがよいと思います。
Q4	
Q5	最初に，指定調査機関とはどういうものか（定義）を書いて，「（電子署名法 17 条以下）」という具合に条文を参照するとよいと思います。
Q6	回答文に主語がありません。「指定調査機関は」または「電子署名・認証センターは」の趣旨だと思いますので，主語を明記してください。
Q7	
Q8	文章がやや変です（「事実はありません」というのは，こういう Q&A にはそぐわないと思います）。「平成２３年×月×日時点で，現行認定認証業務の自己署名証明書は，IE の証明書ストアにルート証明書として登録されていません」ぐらいでいかがでしょうか。

7．全体に対して

ご意見

4.2 認定認証事業者からの問い合わせ Q&A

4.1.1 4.2.1 認定認証事業者からの問い合わせ Q&A（電子署名･認証制度全般編）

(諮問委員からのご意見)

a)手塚委員

１．電子署名･認証制度全般

ご意見	
Q1	回答はこれでよいと思います。利用者署名符号を代理人が管理する場合についても回答を考えておく必要があると考えます。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
Q5	特に問題なし。
Q6	回答はこれでよいと思います。電子証明書の有効期限が切れたときの効力についても言及するほうが良いと思います。
Q7	特に問題なし。

２．その他

	ご意見
Q1	特に問題なし。

全体に対して

ご意見
回答は良く書かれていると思います。あえて言うならば、専門的な言葉が出てくるのはやむを得ないが、相手の知識レベルに合わせた回答をするように心がけていただきたい。

b)早貸委員

１．電子署名･認証制度全般

ご意見	
Q1	電子署名・認証業法の施行時の議論として、利用者署名符号の管理に関する利用者側の要件等については同法で規律することができなかったので、事業者の認定基準のなかに、事業者に、顧客である利用者に対して、利用者署名符号の適切な管理が可能となるような環境を提供したり、厳重な管理の必要性に関する認識をもたせるための措置を講じたりすることを求める形で、入れ込むことされたと記憶しているが、その場合における利用者署名符号の管理方法としては、利用者自らが管理する方法だけでなく、利用者署名符号のうち署名鍵に該当する部分を認証局やRAその他のサービス提供事業者が安全に保管し、その署名鍵を発動させるための符号を利用者のみが管理すると言う方法も念頭に置かれていたと記憶。 なので、認証局その他の組織が鍵を預かる場合でも、（鍵が安全に保管されていることはもちろん必要ですが、）その鍵を起動させるために別の符号が必要なシステムになっていて、その起動させるための符号を利用者のみ（認証局は保管しない）が保管している等、利用者のみが電子署名を行うことができると言える環境が構築されてるのであれば、そのような業務の提供もあり得るものと考えます。
Q2	
Q3	この質問は、指定調査機関の役職員の秘密漏えいの文脈で回答すべき問題ではなく、情報公開請求との関係で回答すべき問題なのではないでしょうか？ 結論から言うと、指定調査機関が「行政機関の保有する情報の公開に関する法律」または「独立行政法人等の保有する情報の公開に関する法律」の適用を受ける行政機関または独立行政法人でない場合には、個人情報保護法その他の個別の法の規定に基づく場合以外には、保有している情報の開示請求に応じる義務はない。ただし、指定調査機関が監督官庁に提出した報告書については、それらの省庁に対すして開示請求があれば、行政機関の保有する情報の公開に関する法律が定める不開示情報（同法第5条）に該当しない限り各省庁が開示の義務を負うので、必要であれば、監督官庁に対して情報開示請求をすればよいと考えます。
Q4	
Q5	電子署名・認証業法の定める事項を越えた問題ではありますが、使用の範囲を、「認定認証事業者が当該業務の利用者に限定して個別に提供する通信サービス」に限る必要性（合理性）がわかりません。
Q6	説明資料の添付が見当たらなかったので、想定しているシステムの内容が分かりませんが、回答に書いていること自体には問題はないかと。
Q7	

２．その他

ご意見	
Q1	

全体に対して

ご意見

c)宮内委員

１．電子署名･認証制度全般

ご意見	
Q1	「……第三者が容易に当該署名符号により電子署名できないようになっている必要があります。」のところに，括弧書きで，認証局もここでいう第三者に含まれる旨を記載すると，論旨がより明確になると思います。
Q2	特に問題ありません。
Q3	特に問題ありません。
Q4	最初のパラグラフは，文章が若干長いので，「……が行われることが求められます」は「……の実施が求められます」にしてはいかがでしょうか。
Q5	最初のパラグラフの文章に重複があって趣旨が不明確になっているように思います。必ずしも真意を反映できていないかもしれませんが，例えば，「認定認証業務の利用者署名符号を電子署名以外の用途に用いることに関して、認定認証業務の利用者の便宜を図るための利用が認められています。したがって，認定認証事業者が当該業務の利用者に限定して個別に提供する通信サービスにおいて、当該認定認証業務に係る電子証明書を SSL 通信に使うことは可能です。」という書き方はどうでしょうか。 なお，これは確認ですが，SSL のクライアント認証の実態は，送信メッセージに対するデジタル署名なので，署名用の鍵ペアを用いても問題はないと言うことですね(一般論としては，署名用の鍵をエンティティ認証に使うことは望ましくありませんので）。
Q6	特に問題ありません。
Q7	真偽の確認に使う電子証明書を「電子証明書Ａ」，新たに発行する電子証明書を「電子証明書Ｂ」とした場合，施行規則５条２項に記載される電子証明書は，以下のように解釈されるものとおもいます。 --- 現に電子証明書Ａを有している利用者が当該電子証明書Ａの発行者に対して新たな電子証明書Ｂの利用の申込みをする場合において、当該申込みに係る電子証明書Ｂの有効期間が前項に規定する方法により当該利用者の真偽の確認を行って発行された電子証明書Ａ【正確に言えば初回発行の電子証明書】の発行日から起算して五年を超えない日までに満了するものであるときは、同項の規定にかかわらず、当該発行者は、当該利用者が現に有している電子証明書Ａに係る電子署名により当該利用者の真偽を確認することができる。 --- つまり，②の解釈で正しいと考えます。
２．その他	
ご意見	
Q1	係り受けが少し変です(「ホームページ内に……使用，……リンクについては」という文章になっています）。冒頭を「認証局のホームページにおける」としてはいかがでしょうか。

全体に対して

ご意見
特にありません。

4.1.2 4.2.2 認定認証事業者からの問い合わせ Q&A（認証業務の用に供する設備編）

(諮問委員からのご意見)

a) 手塚委員

１．認証設備関連

１，１認証設備室

ご意見	
Q1	内容的には、特に問題はないと存じますが、関連法令等が多岐にわたるため、その参照先を示していただいておりますが、消防法に関しても参照先を示しておくのがよろしいかと存じます。
Q2	特になし。
Q3	特になし。
Q4	特になし。
１．２．入退出管理システム	
ご意見	
Q1	特になし。
Q2	管理用ハードウェアの定義が不明であるので、明確にすべきである。その際、Q1 との関係を分かりやすくすべきである。
１．３．認証業務用設備	
1.3.1 軽微な変更（施行規則第九条）	
ご意見	
Q1	特になし。
Q2	特になし。
1.3.2 ハードウェア更改（変更認定が必要な場合）	
ご意見	
Q１	特になし。
1.3.3 ハードウェアの廃棄または機器増設	
ご意見	
Q１	「○○であれば」と書かれているが、これはまずい表現であるので、改善すべきである。
Q2	特になし。
1.3.4 ソフトウェアのバージョンアップ及び設定変更	
ご意見	
Q１	特になし。
Q2	特になし。
Q3	特になし。
1.3.5 認証設備室と登録用端末室(あるいは IC カード発行室)とのネットワーク接続	
	ご意見

Q１	特になし。
Q2	特になし。
Q3	特になし。
1.3.6　その他	
ご意見	
Q１	特になし。
１．４．IDS(侵入検知システム）機器の更改	
ご意見	
Q1	特になし。
Q2	特になし。
１．５．映像記録装置	
1.5.1　遠隔監視装置	
ご意見	
Q1	特になし。
Q2	特になし。
Q3	「お問い合わせいただいた範囲内」と書かれているが、これがどの範囲なのか不明確なので、明確にすべきである。
1.5.2　映像記録装置	
ご意見	
Q1	「お問い合わせいただいた資料の範囲内」と書かれているが、これがどの範囲なのか不明確なので、明確にすべきである。
Q2	特になし。
Q3	「○○の範囲内において」と書かれているが、これはまずい表現であるので、改善すべきである。
Q4	特になし。
Q5	「望ましい処置」は、文章的に「完全消去を実施した後に物理破壊する」と「物理破壊する」のどちらに掛りますか。後者に読めるようにするべきであると考えます。
Q6	特になし。
２．登録用端末設備室	
2.1 登録用端末室	
ご意見	
Q1	特になし。
Q2	特になし。
Q3	「特殊な方法を用いなければ」とありますが、「特殊な方法を用いず」とした方が良いように考えます。
2.2 登録用端末設備	
ご意見	

Q1	特になし。
Q2	特になし。
Q3	特になし。
Q4	特になし。
Q5	特になし。
３．その他	
3.1 リポジトリ	
ご意見	
Q1	特になし。
Q2	特になし。
Q3	特になし。
3.2 NTP(時刻同期)	
ご意見	
Q1	特になし。
3.3 ログ収集	
ご意見	
Q1	特になし。
Q2	特になし。
3.4 認証業務用設備等の災害の被害を防止するために必要な措置	
ご意見	
Q1	特になし。
3.5 セキュリティ対策	
ご意見	
Q1	特になし。
Q2	特になし。
3.6 認証業務用設備以外の軽微な変更	
ご意見	
Q1	特になし。
Q2	特になし。
Q3	特になし。
Q4	特になし。
Q5	特になし。
Q6	特になし。
Q7	特になし。

全体に対して
ご意見

Q&A であることから、Q の内容説明が明確でないところがあり、A の回答内容が不明確となるものもあったので、その点、もっと丁寧に Q の内容を書き、A の回答をするほうが誤解を招かないと考えます。

b) 早貸委員

１．認証設備関連

１，１認証設備室

ご意見	
Q1	特になし
Q2	特になし
Q3	特になし
Q4	特になし
１．２．入退出管理システム	
ご意見	
Q1	特になし
Q2	特になし
１．３．認証業務用設備	
1.3.1　軽微な変更（施行規則第九条）	
ご意見	
Q1	回答の第2段落が「またその他のサーバにつきましては」から始まるのですが、「その他のサーバ」というのは何を指しているのか不明です。
Q2	「ハードウエア、ソフトウエアの更改及び新規追加」というと、ものすごく範囲が広いと思うのですが、この書き方だと、入れ替えや追加によって、セキュリティその他の要件がデグレードしていないことが担保されていない、機能を縮小させたり、機能が追加されるけれどもセキュリティ面ではレベルが下がる場合も含めて、申請不要と言っているように読めるのですが、そういう趣旨ではないですよね？
1.3.2　ハードウェア更改（変更認定が必要な場合）	
ご意見	
Q１	
1.3.3　ハードウェアの廃棄または機器増設	
ご意見	
Q１	書きかけでしょうか？
Q2	
1.3.4　ソフトウェアのバージョンアップ及び設定変更	
ご意見	
Q１	バージョンが上がる＝同等以上の機能とは限らないので、その点を留保しておく記載が必要だと思います。
Q2	CRLの生成・更新プログラムを改修することによって、配付ポリシーが影響を受ける（結果的に変更になる）場合は、法4条2項3号に該当する可能性があるので、配付ルールやポリシーに影響が生じないことを条件にする必要があるように思われますが、いかがでしょう。
Q3	Q１と同様、バージョンアップ＝同等以上の機能とは限らないので、その点の留保が必要だと思

	います。
1.3.5　認証設備室と登録用端末室(あるいはICカード発行室)とのネットワーク接続	
ご意見	
Q１	「直接ネットワーク接続」の趣旨が不明ですが、このネットワークがインターネット等をいうものであれば、FWなしにすることは問題あると思いますが・・・。何か環境に関する前提が設問等から飛んでしまっているのでは？
Q2	リプレースすること＝同等以上の機能とはかぎらないので、その点の留保が必要。
Q3	設問にある「認証設備質間のネットワーク接続」が、回答ではいきなり「認証設備室が設置されている建物内における接続変更」で回答されていますが、設問にはそのような前提の設定がない（インターネット経由かもしれない、というように読めます。）ので、回答に無理があるのでは？
1.3.6　その他	
ご意見	
Q１	ラックを移動することで、監視カメラ（監視カメラにより監視が業務の運営に組み込まれている場合）に死角が発生したりする可能性があるので、そのような問題が生じないことを留保しなければならないのでは？
１．４．IDS(侵入検知システム）機器の更改	
ご意見	
Q1	ソフトウエアのバージョンアップ＝同等機能以上とは限らない点に関する留保が必要
Q2	調査表の項目が別だとか、主務省に報告済だとかということを理由にするのは、合理的ではないと思いますが。
１．５．映像記録装置	
1.5.1　遠隔監視装置	
ご意見	
Q1	特になし
Q2	特になし
Q3	「お問い合わせいただいた範囲内」が何なのかわかりません。
1.5.2　映像記録装置	
ご意見	
Q1	添付資料の範囲内、が分かりません。
Q2	
Q3	○○の部分次第。
Q4	
Q5	
Q6	
２．登録用端末設備室	
2.1 登録用端末室	
ご意見	

Q1	変更してもよいと思いますが、変更申請は不要でしょうか？不要にするのであれば、カードの発行及び管理について、規定を求めるだけではなくて、どういうように規定すべきか（具体的な手法ではなく、無権限者に対する発行が行われないように、とか、第三者が勝手にICカードを利用することができないように、とか、といった明確かつ適切に規定すべき事項を留保しておく必要があるのではないでしょうか？
Q2	中断の３つの箇条書きが前後とどうつながるのか、多少言葉の補足が必要であると思います。
Q3	この設問は変更申請の要否にかかる設問ではなく、使ってよいかと聞かれているという理解ですね？
2.2 登録用端末設備	
ご意見	
Q1	「望ましい」で足りますか？
Q2	
Q3	設問からは、どういう状況からの変更なのかが読み取れません。
Q4	「望ましい」で足りますか？
Q5	
３．その他	
3.1 リポジトリ	
ご意見	
Q1	
Q2	ソフトウエアのバージョンアップ＝必ずしも同等以上の機能とは限らないので、その点の留保。
Q3	同上
3.2 NTP(時刻同期)	
ご意見	
Q1	
3.3 ログ収集	
ご意見	
Q1	
Q2	
3.4 認証業務用設備等の災害の被害を防止するために必要な措置	
ご意見	
Q1	
3.5 セキュリティ対策	
ご意見	
Q1	
Q2	
3.6 認証業務用設備以外の軽微な変更	
ご意見	

Q1	特になし
Q2	
Q3	
Q4	
Q5	
Q6	
Q7	

全体に対して

ご意見

c） 宮内委員

１．認証設備関連

１，１認証設備室

	ご意見
Q1	①の２番目の文が完結していません。 「消防法……」を確認するための「……」及び「消防用設備……」を確認するための「検査結果通知書」がこれにあたります。 というような文章にしてはいかがでしょうか。 ②の「イ」ないし「ハ」は，条文のコピーのようですが，条文をそのまま掲載する意義はなんでしょうか？
Q2	
Q3	Q3 は「該当しないものと思われます」，Q4 は「変更には該当せず」となっていて表現が微妙にちがいます。できれば統一するべきだと思います。
Q4	

１．２．入退出管理システム	
	ご意見
Q1	最後のパラグラフ（関連法令の直前）の，「一号二」は「ニ」（かたかな）ですね（二箇所あります） 関連法令のうち，指針４条１号ロ，７条２号ホ，13 条１号は，本文中で関連する事項すらも扱っていないので，ここに書くのは不適当だと思います。なお，規則６条 15 号イも，関係は薄いので消しても良いと思います。
Q2	関連法令は，法４条２項２号だと思います。（法４条２項２号に当たらない以上，規則９条は無関係です）

１．３．認証業務用設備	
1.3.1 軽微な変更（施行規則第九条）	
ご意見	
Q1	
Q2	
1.3.2 ハードウェア更改（変更認定が必要な場合）	
ご意見	
Q１	HSM の性能次第では，規則９条の適用があるのではないでしょうか。
1.3.3 ハードウェアの廃棄または機器増設	
ご意見	
Q１	「○○」が残っていますので，修正してください。
Q2	
1.3.4 ソフトウェアのバージョンアップ及び設定変更	
ご意見	

Q１	「……変更 j が生じないとのことなので」は，「……変更が生じないのであれば」とすべきです。（変更が生じないとは，質問文に書かれていないため）
Q2	本 Q&A では，バージョンアップやパッチは一貫して，法 4 条 2 項 2 号又は 3 号に該当するという前提に立って，規則 9 条の適用を問題にしています（1.3.4 の Q1,Q3 など）。それに対し，本問では，プログラムの改修は法 4 条 2 項 2 号にも 3 号にも該当しないとしているのですが，これは，バランスを欠くように思います。
Q3	
1.3.5　認証設備室と登録用端末室(あるいは IC カード発行室)とのネットワーク接続	
ご意見	
Q１	Q1 の末尾の「問題ないでしょうか？」は，1.3.4 の各 Q と同様に「変更認定の申請が必要でしょうか？」として統一をとるのがよいと思います。
Q2	Q2 のルータの更改は規則 9 条を適用しているので，法 4 条 2 項 2 号又は 3 号に該当するということになりますが，これに対して，Q3 では，ネットワーク接続の変更は法 4 条 2 項 2 号に該当しないとしています。ルータのリプレイスが法 4 条 2 項にあたるのに，回線の種類の変更があたらないというのは，バランスを欠いているように思います。
Q3	
1.3.6　その他	
ご意見	
Q１	
１．４．IDS(侵入検知システム）機器の更改	
ご意見	
Q1	
Q2	関係法令は，規則 4 条 2 号及び指針 5 条 1 号ではないでしょうか。（電気回線を通じた不正アクセスの話をしているように思えます）
１．５．映像記録装置	
1.5.1　遠隔監視装置	
ご意見	
Q1	変更認定が不要な理由は何でしょうか。法 4 条 2 項にあたらないからですか，それとも，法 4 条 2 項にはあたるものの規則 9 条の適用があるということでしょうか。
Q2	「施行規則 4 条各号」とありますが，関係するのは 5 号だけではないでしょうか。
Q3	関連法令は，法 4 条 2 項 2 号ではないでしょうか。
1.5.2　映像記録装置	
ご意見	
Q1	
Q2	「規則 4 条各号」は 3 号だけだと思います。

Q3	「○○」が残っていますので，修正してください。 「第四条各号」は三号だけだと思います。
Q4	この変更は規則 9 条にはあたりません。規則 9 条は「同一室内における」が要件となっているところ，この変更は室外に移動しているためです。ですから，この変更が法 4 条 2 項にあたるかどうかはともかく，規則 9 条は適用できないはずです。 なお，「第四条各号」は三号だけだと思います。
Q5	文章の問題だけです。 冒頭の部分は「……映像に，……が記録されている場合は」とすべきです。 次の文章の冒頭は，「該当する場合には，」とすると良いと思います。
Q6	
２．登録用端末設備室	
2.1 登録用端末室	
ご意見	
Q1	これは，規則 9 条が適用されるということでしょうか？
Q2	箇条書きの直前に「なお，以下の点についても注意が必要です。」という文を入れてもらえませんか。
Q3	
2.2 登録用端末設備	
ご意見	
Q1	
Q2	
Q3	法 4 条 2 項 2 号の事項にあたらないのであれば，「安全性を向上させる措置」かどうかは問題にならないはずです。これが問題になるのは規則 9 条の適用を可否を判断する場合ですので，記述の一貫性を欠いているように思います。
Q4	
Q5	
３．その他	
3.1 リポジトリ	
ご意見	
Q1	
Q2	
Q3	
3.2 NTP(時刻同期)	
ご意見	
Q1	
3.3 ログ収集	

ご意見	
Q1	規則 9 条により申請不要ということでしょうか。
Q2	
3.4 認証業務用設備等の災害の被害を防止するために必要な措置	
ご意見	
Q1	
3.5 セキュリティ対策	
ご意見	
Q1	
Q2	
3.6 認証業務用設備以外の軽微な変更	
ご意見	
Q1	
Q2	規則 9 条により申請不要ということでしょうか。
Q3	規則 9 条は，同一室内のみが対象なので，室外に設置する場合には適用できません。
Q4	「変更は可能である」→「変更認定の申請は不要である」とすべきです。 「どちらの方式でも」という記載がありますが，この記載が何を指しているか不明です。 「PIN 印刷仕組みの変更は必ずしも業務運用上の変更とはならず」とあります。どういう場合に業務運用上の変更になるのか記載するべきです。
Q5	
Q6	
Q7	法 4 条 2 項各号にあたらないので，関係法令に規則 9 条を書くのは不適切です。

全体に対して

ご意見
法 4 条 2 項 2 号又は 3 号に該当する場合には変更申請が必要ですが，そのような場合でも「同一室内における……とする」が成立するときには，例外的に変更認定が不要になるという条項が施行規則 9 条です。したがって，施行規則 9 条が適用されるということは，法 4 条 2 項 2 号又は 3 号に該当することが前提です（判決書でしたら，「法 4 条 2 項 2 号又は 3 号に該当するかどうかはともかく，規則 9 条の条件に該当するので，変更認定は不要と認められる」という書き方になるのでしょうが，Q&A は，そういう書き方はすべきでないと思います)。 この点に混乱があるのではないか，という箇所がいくつかあります。それぞれの箇所で指摘しておきましたのでご覧ください。 なお，この Q&A においては，ソフトウエアのバージョンアップ及びパッチは，法 4 条 2 項に該当するが，規則 9 条が適用になるので変更認定不要(1.3.4 Q1，Q3 等)という考え方で一貫しているのですね(確認です)。

4.1.3 4.2.3 認定認証事業者からの問い合わせ Q&A（利用者の真偽確認編）

(諮問委員からのご意見)

a）手塚委員

1．利用者の真偽確認資料

	ご意見
Q1	具体的にどの証明書ならよいのかを明示する必要があるので、真偽確認に使える証明書が新たに判明した時には、その都度公表かつ明示するようにすべきである。
Q2	具体的にどの証明書ならよいのかを明示する必要があるので、真偽確認に使える証明書が新たに判明した時には、その都度公表かつ明示するようにすべきである。
Q3	特に問題なし。

2．真偽確認方法

	ご意見
Q1	書かれていることは特に問題ないと思いますが、さらに「公的個人認証サービスの電子証明書」の失効チェックができることが条件となることを表記すべきである。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
Q5	特に問題なし。
Q6	特に問題なし。

3．漢字の置き換えについて

	ご意見
Q1	特に問題なし。

4．その他

	ご意見
Q1	特に問題なし。
Q2	特に問題なし。

全体について

	ご意見
	・真偽確認の方法と証明書については、様々な提案が出てくると思われますので、その都度精査して、応えることが重要であり、その結果を他の認定認証事業者にもその情報を共有してもらう必要があると考えます。 ・住所や氏名等の表記においては、表記方法や漢字表記に揺らぎが出てきますので、その取扱いについては、常に例示を示し、認定認証事業者が混乱しないようにする必要があると考えます。

b) 早貸委員

1．利用者の真偽確認資料

	ご意見
Q1	「広域交付住民票」は、「住民票の写し」であるので、「住民票の写し」と同様に取扱う旨を説明書類に記載するという表記は成立しないのではないでしょうか？　●●と同様に取り扱うというのは、異なるものであることを前提に同様に扱うということ意味だと思うので。あり得るとすれば「住民票の写し」の説明として、「（広域交付されたものを含む。）」との説明を付加する、ぐらいでしょうか？ 一方「住民票記載事項証明書」のほうは、住民票とは異なるものですので、こちらは、「住民票の写し」と同様に取り扱う旨の規定が必要であると考えます（原案の書きぶりで可。）。ただし、設問には、住民票記載事項証明書のことは全く出てきていないので、回答の 3 段落目は、「また」ではなく、「なお、」で始めるべきではないかと思料します。
Q2	
Q3	本人確認は、利用の申し込みをした時点で行うものであり、「本人」を確認するために行うものであって、発行した電子証明書は国内での利用に限って使えるという制約もないと思うので、なぜに失効させる必要があるのか、わかりません。滞在期間は延長されることもあります（というか更新され続ける場合のほうが実態としては多いかも。）ので、スナップショットで、あるタイミングの滞在期間をとらえて、電子証明書の有効期間とリンクさせる必要はないと考えます。

2．真偽確認方法

	ご意見
Q1	
Q2	設問の意味が伝わりにくいと思います。回答でいきなり本人確認方法を追加する話になっていて、Q と A がかみ合っていない気がします。対面での確認の場合でも、「住民票の写しの提出は必要。運転免許証は提示で可。」ということが読み取れないですね。
Q3	「読み方が不明となった場合」というのは、いったんこの読み方だと思っていたものが、後発的に不明になったという場合でしょうか？　どういう場合かわかりづらいですが・・・。もし、利用の申し込みの際に提出または提示された書類等に、読み仮名の記載がないために、読み方が提出書類から確認できないという趣旨であれば、日本の戸籍制度等は、漢字の読みを登録させる制度にはなっていないので、本人が読み方を決めることで問題ないはず、です。・・ので読み方が分からない場合には、本人の申請どおりに取り扱うほかなく、提出資料中に、申請にかかる読み方とは異なる読み方での登録がある場合には、その読み方と異なる読み方での証明書の発行は難しいということではないかと。
Q4	住所は、電子証明書の記載事項ではないので、利用申込書の記載が問題になるだけであれば、住民票の記載とのと都合により同一人物であることの確認ができる程度に、また郵便物等の送付がちゃんとできる程度に、表記ぶりが一致していればよいのではないでしょうか？
Q5	同上
Q6	同上

3．漢字の置き換えについて	
	ご意見
Q1	

4．その他	
	ご意見
Q1	利用申込書への記載事項についていえば、Q4 に同じ。
Q2	

全体について

	ご意見

c) 宮内委員

1．利用者の真偽確認資料

	ご意見
Q1	内容に問題はありませんが，なかなか結論に至らないので読みにくいと思います。 最初に， 「広域交付住民票」は，……「住民票の写し」して扱ってよいと考えます。その理由は以下のとおりです。 と書いて，その理由（現在の第１パラグラフ）を書くのがよいと思います。
Q2	特に問題ありません。
Q3	事実として滞在期間を超えた場合に失効するという趣旨はこれでよいと思いますが，その事実を確認する責任を認証局が負うのでしょうか？ つまり，滞在期間が延長されたか否かが不明な状況で， ①本人が滞在期間延長を認証局に届け出ない限り，元の滞在期間の満了時に電子証明書を失効する ②認証局が滞在期間が実際に終了していることを確認した上で電子証明書を失効する のいずれの趣旨でしょうか？ ここは明確に記載するのが良いと思います。

2．真偽確認方法

	ご意見
Q1	特に問題ありません。
Q2	第 2 文が質問文と整合しません。Q2 には，従来の真偽確認方法を変更するとの文言はありません。
Q3	第 2 文（一致確認手順に他の……）の冒頭部分を「認定取得後に一致確認手順に他の資料を追加しても」とした方が，意味が明確になると思います。
Q4	第１パラグラフの末尾は，「容認されていないため，置き換えられません」とすべきです(質問は可能かどうかであって，通達で容認されているかどうか，ではありません)。 第２パラグラフは，意味がとりにくいです。後半の部分を「……が同一とみなせるかどうかを判断するツールにおいて，ハイフンをスペースに置き換えたものを同一と判断しないように規定し，業務を実施してください」としてはいかがでしょうか。
Q5	質問文中の例の末尾に「…○」という記載がありますが，これはどういう意味でしょうか。 第１パラグラフの「従来通りの解釈・運用」はどういう意味でしょうか。同一とみなしてはならない，という意味であれば，そのように記載した方がよいと思います。 第２パラグラフの中ほどの「「住民票の写し」においては」は「「住民票の写し」において」の誤りだと思います（「は」が余計です）。
Q6	特に問題ありません。

3．漢字の置き換えについて

	ご意見

Q1	第３パラグラフ(法務省ホームページ……）が難しく，理解しにくいと思います。 ここで言いたいことは，「JIS 第１，第２水準に含まれない文字は，法務省戸籍統一文字情報の該当文字の記載中の「親字・正字」に置き換えを行っても良い」ということだと思います。これと同等のことが書かれているのだと推察しますが，十分な事前知識のない読者には分かりにくいと思います。 まず，Q1 を「住民票の写しに記載の文字が，JIS の第 1 水準，第 2 水準に含まれない場合の置き換えは，どのように行えばよいのでしょうか」とした上で，第 3 パラグラフを以下のようにしてはいかがでしょうか。 --- JIS 第 1 水準，第 2 水準に存在しない文字については，「法務省 戸籍統一文字情報」の該当文字の記載中の「親字・正字」に置き換えることが可能です。「法務省 戸籍統一文字情報」は，「戸籍手続オンラインシステム構築のための標準仕様書」における選定基準において選定されたものですので，これを漢字置き換えの根拠とできるためです。

4．その他

	ご意見
Q1	「誤字俗字・正字一覧表」は，「平成 16 年 10 月 14 日法務省民一第 2842 号通達」だと思います。これも「通用字体……（平成……）」と同様，括弧書きで記載すべきです。 同じパラグラフの「同一と判断されると思いますが」は，判断主体が不明ですので，「同一と判断できますが」あるいは「同一と判断することができますが」とすべきだと思います。（それとも，将来，裁判所において同一と判断されると思う，という趣旨でしょうか。そうであれば，「裁判では」と書くべきです）。
Q2	特に問題ありません。

全体について

	ご意見
	特にありません。

4.1.4 4.2.4 認定認証事業者からの問い合わせ Q&A（認証業務の実施方法編）

(諮問委員からのご意見)

a) 手塚委員

１．規定改訂関連

１，１認証事業者の社名等の変更に伴う規程の改訂

ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
Q3	指摘事項に対する回答が書かれていないように思いますので、追記が必要に思います。
Q4	特に問題なし。
Q5	特に問題なし。
Q6	特に問題なし。
２．帳簿の変更 ２．1．利用申込書等の変更	
ご意見	
Q1	修正印を押すことを必須とするのかどうかが不明確な表現であると思いますので、「分かるようにしてください。」を「必ず分かるようにしてください。」に表現を変更したほうが良いように思います。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
Q5	特に問題なし。
２．２．認証局内部の帳簿の変更	
ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
Q3	二重線ではまずいといって回答しているが、どうすればよいのかを答えていないので、答えるように した方が良いと思います。
Q4	特に問題なし。
Q5	設問なし。
３．電子証明書格納媒体	
３．１　IC カード	
ご意見	
Q1	特に問題なし。
Q2	特に問題なし。

Q3	特に問題なし。
３．２　USB メモリ／ＣＤ－ＲＯＭ	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
Q3	特に問題なし。
３．３　ＰＫＣＳ１２＃	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
３．４　複数枚発行の電子証明書	
Q1	特に問題なし。
４．委託契約関連	
４．１．外部委託契約の範囲	
ご意見	
Q1	特に問題なし。
Q2	特に問題なし。
４．２．委託先(再委託)の変更	
４．２．１業務委託	
ご意見	
Q1	特に問題なし。
４．２．２　委託契約の変更	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
Q3	特に問題なし。
Q4	特に問題なし。
４．２．３　派遣契約	
Q1	特に問題なし。
４．２．４　業務委託管理	
Q1	特に問題なし。
５．個人情報の取扱い	
ご意見	
Q1	特に問題なし。
Q2	運用規定(CP/CPS)に記載されている場合は運用規定が調査対象になるため個人情報の取扱いに関する記載事項も調査対象になると考えるが、「利用者同意書」となると調査対象にならないので、問題ではないかと考えますが、いかがでしょうか。
Q3	特に問題なし。
Q4	利用者の同意を得ているときは問題ないとの解釈であると理解しますが、それでよろしいでしょうか。

Q5	特に問題なし。
６．利用者へのサービスの変更	
ご意見	
６．１　サービス停止	
Q1	特に問題なし。
６．２　電子証明書の有効期間	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
６．３　利用申込書	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
Q3	特に問題なし。
６．４ 電子証明書の発行対象者	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
６．５ 電子証明書の一時停止	
Q1	一時停止・一時停止解除の対象が、認証局が発行した全部の電子証明書を対象としているのか、それとも特定の個人を対象にしているのかで違いがあると思います。この点を高所した記述にすべきであると考えます。
Q2	特に問題なし。
７．業務体制	
ご意見	
Q1	特に問題なし。
Q2	変更認定の申請が要るのか要らないのかが分かりにくいので、分かるようにした方が良いと思います。
８ 鍵更新	
ご意見	
Q1	前提条件を明確に記載しないといけないと思います。つまり、電子認証システムが１式しかない条件下での記載であることを明確にするようにしていただきたいと思います。
Q2	特に問題なし。
９．業務廃止	
ご意見	
Q1	特に問題なし。
１０．その他 １０．１　プロファイル	
ご意見	
Q1	特に問題なし。

Q2-1	特に問題なし。
Q2-2	特に問題なし。
Q3	特に問題なし。
１０．２　リポジトリ	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
Q3	特に問題なし。
１０．３　業務運用者用電子証明書	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
１０．４　認証事業者による利用者署名符号の生成措置	
Ｑ１	特に問題なし。
Ｑ２	特に問題なし。
Q3-1	特に問題なし。
Q3-2	特に問題なし。
Q3-3	特に問題なし。
１０．５　その他	
Q1	どこに問い合わせをすればよいかを書く必要があると思います。

全体に対して

ご意見
全体として、大変丁寧に質問に対して回答されていると思います。 文章を読んでやっと変更認定等の申請をする必要があるのかないのかが分かる文章が多く見受けられます。 できれば、回答の最初に必要か必要でないかを明記して、それから理由を述べるようにした方が、読み手にとっては分かりやすいと思います。

b) 早貸委員

１．規定改訂関連

１，１認証事業者の社名等の変更に伴う規程の改訂

ご意見	
Q1	URI → URL
Q2	
Q3	
Q4	他の設問の回答とは粒度が異なる回答のように見受けられます。
Q5	
Q6	

２．帳簿の変更

２．1．利用申込書等の変更

ご意見	
Q1	
Q2	
Q3	
Q4	
Q5	

２．２．認証局内部の帳簿の変更

ご意見	
Q1	
Q2	
Q3	
Q4	
Q5	

３．電子証明書格納媒体

３．１　IC カード

ご意見	
Q1	「追加されるメーカの IC カード」・・・という記載は固有の製品に関する記述なのだと思いますが、 この記載では Q&A として独立できていないと思われます。
Q2	初期不良の原因が認証局の責に帰すべきものである場合に、利用者の申出に実印の押印を求める合理性が分からないのですが。
Q3	

３．２　USB メモリ／ＣＤ－ＲＯＭ

Q１	

Q２	
Q3	設問の文章中に、何を直接印刷するのかの記載が欠けているように見受けられます。
３．３　ＰＫＣＳ１２＃	
Q１	
Q２	
３．４　複数枚発行の電子証明書	
Q1	
４．委託契約関連	
４．１．外部委託契約の範囲	
ご意見	
Q1	
Q2	「登録業務のすべて」の言葉が意味するところがずれているのかもしれませんが、登録局と認証局が分かれている場合に、だれが認定申請をするかという問題なのでしょうか？
４．２．委託先(再委託)の変更	
４．２．１業務委託	
ご意見	
Q1	
４．２．２　委託契約の変更	
Q１	
Q２	
Q3	
Q4	
４．２．３　派遣契約	
Q1	委託を解除しても「人員管理方法」に変更がない場合はあり得ないのではないでしょう。
４．２．４　業務委託管理	
Q1	
５．個人情報の取扱い	
ご意見	
Q1	
Q2	
Q3	
Q4	
Q5	自ら提起した訴訟における立証のために行う情報提供は、司法からの要求に応じた情報提供とは言わないと思います。
６．利用者へのサービスの変更	
ご意見	
６．１　サービス停止	

Q1	
６．２　電子証明書の有効期間	
Ｑ１	
Ｑ２	
６．３　利用申込書	
Ｑ１	
Ｑ２	
Q3	
６．４ 電子証明書の発行対象者	
Ｑ１	
Ｑ２	
６．５ 電子証明書の一時停止	
Q1	
Q2	
７．業務体制	
ご意見	
Q1	最小限の人数というのは、事故対応等の平時とは異なる業務をも見込んだ上での最小限という趣旨でよいでしょうか？
Q2	
８ 鍵更新	
ご意見	
Q1	
Q2	
９．業務廃止	
ご意見	
Q1	
１０．その他 １０．１　プロファイル	
ご意見	
Q1	
Q2-1	
Q2-2	
Q3	
１０．２　リポジトリ	
Ｑ１	
Ｑ２	
Q3	「ご提示いただきました…変更案」が不明なので、Q&A として独立できていないと思われます。

１０．３　業務運用者用電子証明書	
Ｑ１	
Ｑ２	
１０．４　認証事業者による利用者署名符号の生成措置	
Q1	
Q2	
Q3-1	
Q3-2	
Q3-3	
１０．５　その他	
Q1	

全体に対して

ご意見

c) 宮内委員

１．規定改訂関連

１，１認証事業者の社名等の変更に伴う規程の改訂

ご意見	
Q1	
Q2	
Q3	「提案事項」についてのみ回答していて，「指摘事項」ついて回答していないようですので，こちらの回答も記載してください。 関係法令で，4 条 2 項 2 号が 2 回あります。片方は 3 号だと思います。
Q4	設備･施設の変更は，本問とは無関係だと思います。 関係法令で，4 条 2 項 2 号が 2 回あります。片方は 3 号だと思います。
Q5	文言を少し直しました。別紙をご覧ください。 【別紙内容】 利用者宛に電子証明書と併せて送付する電子証明書の内容確認マニュアルの修正部分が問い合わせの範囲であれば、電子署名法の対象に該当せず、変更認定の申請は必要ありません。 実施に際しましては、貴認証局の判断の元、当該マニュアルを変更してください。
Q6	「相互認証証明書の有効期間の明確化」はかなり唐突なので，削除してはいかがでしょうか。

２．帳簿の変更

２．1．利用申込書等の変更

ご意見	
Q1	質問文の冒頭部分がわかりにくいので，添付のように修正してはいかがでしょうか。 関係法令の規則 6 条 4 号は，有効期限は 5 年を超えないという条文です。不要ではないでしょうか。 【添付修正内容】 有効期間の異なる複数の種類の電子証明書を発行しようとしています。そのため，電子証明書の有効期間を新たに追加するのですが，その際に、現行の利用申込書に暫定的に有効期間を利用者に追記させることは、問題ないでしょうか？
Q2	
Q3	
Q4	質問文の意味が分かりません。もともと「利用者本人以外からの失効申請」の手続があって，その申請のための添付書類を追加するという趣旨ですか？ それとも，本人以外からの施行申請を新設するという趣旨ですか。 回答文も意味が読み取れませんでした。最初の文は，日本語として正しくないと思います。また，結論として，変更認定は不要だと言っているのでしょうか？ なお，この文は，具体的な CP/CPS を前提として，それについて説明しているようですが，その CP/CPS の内容がわからないため，回答の意味を読み取ることが困難です。また，「CP/CPS に明確に記載されていない場合」と書いていますが，これは組織等からの失効申請の要件を明確にせ

	よということですか？ 「場合」が 2 回重なっているので，とても読みにくいです。 最後の「なお書き」は，質問文との関係がわかりません（質問文の趣旨が不明なため）。
Q5	
２．２．認証局内部の帳簿の変更	
ご意見	
Q1	
Q2	「発行チェックリストの１セットの枚数」とは何のことでしょうか。
Q3	二重線のみの訂正はダメだと書くだけでなく，訂正印が必要だと明記すべきです。
Q4	
Q5	（2.2 に Q5 はありません）
３．電子証明書格納媒体	
３．１　IC カード	
ご意見	
Q1	文章がわかりにくいので修正してみました。別紙をご覧ください。 法 4 条 2 項に該当しないという点について。Q&A の「設備編」では，ソフトウエアのバージョンアップは，法 4 条 2 項にあたるものの規則 9 条により変更認定不要としています。IC カードのバージョンアップが法 4 条 2 項にあたらないという見解は，「設備編」と整合しませんので，調整が必要です。 【別紙内容】 IC カードの仕様は電子署名法の認定基準に明確には定められていませんが、利用者署名符号が安全に格納可能な保存媒体であることが必要です。追加されるメーカの IC カードは、IC カードから端末間のデータ通信の転送プロトコルの定義の一部が異なるものの、それ以外は、現行使用している製品の仕様と変更がありませんから、当該 IC カードを使用することについて、変更認定の申請は必要ありません。
Q2	特初期不良について「……と解されている」とのことですが，誰がそのように解しているのか，根拠となる文献を示すべきです。 第二パラグラフは文章が非常に長いので，別紙のように直すべきだと思います。 第三パラグラフは趣旨がわかりませんでした。帰責性を確認できる資料＋実印押印文書が必要といいたいのでしょうか。今の記載は，「別の手段で確認できる場合には，実印押印文書が必要」という構造になっています（確認できない場合には不要，とも読めます）。
Q3	第二パラグラフの文が非常に長いので，別紙に修正案を載せました。 【別紙内容】 但し、電子証明書に記載されている個人情報が当該認証業務以外の第三者に公開される、又はその恐れがあることについて、予め利用者の同意が必要です。さらに、調査委託契約等において、検査機関に対し、利用者署名符号（秘密鍵）の使用及び利用者署名符号の探査の実行等、利用者及び認証業務のセキュリティを脅かすような行為を行わないことを義務づけ

	る必要もあると考えます。
３．２　USB メモリ／ＣＤ－ＲＯＭ	
Ｑ１	ロジックの構造が不明です。そもそも，電子証明書の格納媒体ではなく，署名鍵(秘密鍵)の格納媒体を問題にすべきだと思います。以下に疑問点を列挙します。 ・規則 6 条 3 号は，署名鍵の受け渡しに関するものなので，電子証明書の格納媒体を論じる本問とは，無関係ではないか。 ・規則 6 条 3 号の 2 は，電気通信回線を通じて検証鍵(公開鍵)を受信する場合に関するものなので，本問とは無関係ではないか。 ・規則 6 条 3 号及び 3 号の２が無関係だとすると，方針第 4，２も無関係になる。
Ｑ２	「同等程度の機能・性能……」の条件のもとで法 4 条にあたらないというのは変です。これは規則 9 条の要件についていっているのではありませんか。 法 4 条にはあたるが，同等程度の機能性能を有するので規則 9 条が適用できる，ということなら理解できます。
Q3	質問と回答が対応していません。修正してみましたのでご覧ください。 【別紙内容】 Q 利用者署名符号の格納媒体の表面への必要情報の記載方法を、必要情報が記載されたラベルを貼付する方法から、直接、必要情報を利用者署名符号の格納媒体である CD-R の表面に記載する方法に変更する場合は、変更認定の申請が必要でしょうか？ A 電子証明書の格納媒体についての変更の場合、安全、確実に利用者に渡す要件により、その媒体の安全性を確認するため、変更認定の申請が必要となる場合があります。 しかし、質問文のように具体的な記載方法を変更しても、利用者署名符号の安全性に影響することはないと思われるますので、変更認定の申請は必要ありません。 実施にあたり、規程及び仕様書等において、必要情報の記載に関する一部の操作手順の変更等について、修正し実施して頂ければと考えます。
３．３　ＰＫＣＳ１２＃	
Ｑ１	「HDD に発行する」には違和感があります。秘密鍵を「発行」とは言いませんし，発行を受けるのは人であって HDD ではありません。「生成した秘密鍵を HDD に格納する」のような表現にしてはいかがでしょうか。 回答文が，案１・案２共通の記載，案２の記載，共通の記載，というように行ったり来たりするので，別紙のように変更するのがよいと思います。また，日をまたがなくても，秘密鍵が HDD に格納されている間は，十分な配慮が必要と思います。
Ｑ２	回答文の最初に「問題ありません」と明記すべきです。 ２～５番目の「・」は本問と無関係に思えます。削除してはいかがでしょうか。
３．４　複数枚発行の電子証明書	
Q1	規則 6 条 3 号の 2 に言及していますが，3 号の 2 は検証鍵の通信回線による送信ですから，本問

	には関係がありません。ここで言及すべきは 3 号だと思います。 第二，第三パラグラフは問われていないことを答えています。これを記載したいのであれば，「送付方法の変更について教えてください」等の別の質問をたてるべきです。
４．委託契約関連	
４．１.外部委託契約の範囲	
ご意見	
Q1	文章がわかりにくいというか，係り受けがよくわかりません。業務の全部の委託が不適当でない理由を端的に示すべきです（今の文章では，何が理由なのかわかりません）
Q2	法 2 条 2 項から直ちに，「可否判断を最終的に行うことが必要」といえるのでしょうか。ここは，もう少し説明を追加して，そのロジックを明らかにしてください。
４．２.委託先(再委託)の変更	
４．２．１業務委託	
ご意見	
Q1	（この Q&A に問題はないですが，章・節の番号が間違っています。それぞれ「4.2」「4.2.1」です）
４．２．２　委託契約の変更	
Ｑ１	
Ｑ２	「委託契約を管理している」とは具体的に何をしているのでしょうか。（委託契約の管理とは，何をすることでしょうか）
Q3	ここの回答自体は正しいと思います。 ただし，分割により，本件の委託業務に関する全ての権利義務を一方の会社が一括して引き継ぐのであれば，そもそも委託契約の変更が不要になると思います（したがって，変更認定も不要）。なぜ，新規に委託契約を締結する方法のみを記載しているのでしょうか。
Q4	冒頭に「変更内容によります」と明記すべきです。
４．２．３　派遣契約	
Q1	委託をやめて直接実施にする場合に，人員管理方法に変更がない，ということは想定しにくいと思います。むしろ，「人員管理方法に変化があれば，変更認定の申請が必要です」という旨の文章に直してはいかがでしょう。
４．２．４　業務委託管理	
Q1	「それを連続して」という記載がありますが，何と何が連続するのでしょうか。複数の担当者の記載を一つの(連続した)ページにまとめる，という意味でしょうか。今のままでは，非常にわかりにくいので表現を工夫するべきだと思います。
５．個人情報の取扱い	
ご意見	
Q1	回答文がわかりにくいので直してみました。別紙をご覧ください。 【別紙内容】 現在の申し込み時の流れのはじめに、個人情報の取扱の条件に同意をいただく処理を挿入

	するだけであり、それ以外にはこれまでの申し込みの流れを変更しない方法なので、特段の問題はないものと思料します。
Q2	
Q3	電子媒体自身を暗号化することはできませんので，「電子媒体内の情報を暗号化」等の表現にすべきです。
Q4	回答文がわかりにくいので直してみました。別紙をご覧ください。 【別紙内容】 認証業務において得た情報を認証局以外の他部門に情報提供することは施行規則第六条十五条への「利用者の真偽の確認に際して知り得た情報の目的外使用の禁止」に該当します。 なお、運用規程（CP/CPS）や利用規程に記載してある個人情報の取扱の記述次第では、認証局の他部門に電子証明書の取得情報を提供することに対して、利用者の同意を得ているとは判断できるケースもありうると思われます。
Q5	全体として，質問者が示した具体的な規程を前提として回答しているように思います。しかし，その規程については質問文に書かれておらず，唐突に回答文で出てくるので，読み手には理解しがたい内容になっています。 当該規程を知らない人にもわかるような内容に修正すべきです。
６．利用者へのサービスの変更	
ご意見	
６．１　サービス停止	
Q1	質問文の趣旨がわかりにくいので，修正すべきだと思います。別紙のコメント欄をご覧ください。
６．２　電子証明書の有効期間	
Ｑ１	質問文，回答文，それぞれ１箇所の表現を修正しました。別紙をご覧ください。
Ｑ２	有効期間の起算点が「可否判断日」である，という根拠条文を明らかにしてください（私は，このような考え方だと知りませんでしたので，ご教示ください）。 規則６条４号は「5 年を超えない」（5 年以下の意）ですから，「5 年未満」は誤りです。 発行承認時から開始時刻までに一定期間をあけるという記載がありますが，これは有効期間の起算点が可否判断日であるという記載と矛盾しているように思います。
６．３　利用申込書	
Ｑ１	
Ｑ２	ワードのすかしのようなものを想定しているのでしょうか。どういうものなのかも，入れる目的は何なのかも，どちらも理解できません。 もう少し説明を入れてください（どういうものなのか，何のために入れるのか）
Q3	「提出された規程の範囲では」といわれても，読者にはわかりません。当事者以外にもわかるように記載してください。
６．４ 電子証明書の発行対象者	

Q１	文章がわかりにくいので修正してみました。別紙をご覧ください。 【別紙内容】 施行規則第五条一項のただし書きの括弧書きの「利用申込者本人が国外に居住する場合においては……」との記載により、海外に居住（在留）されている方への、電子証明書の発行が予定されていることが読み取れます。したがって、電子署名法は、電子証明書発行対象者について、特段の制限を加えていないと解釈できます。 具体的には、住民票の写しや印鑑登録証明書に準ずるものを利用して、真偽確認を実施する必要があると思料いたします。その他、実施に際しては懸念されている、「信書の問題、印鑑証明書の問題、証明書・PIN の受渡の問題、印鑑(サイン)の照合の問題等」について詳細に検討する必要があります。 また、変更認定にあたるか否かの判断を行うには、上記の対応等を踏まえた変更内容を具体的に提示していただく必要があります。
Q２	
６．５ 電子証明書の一時停止	
Q1	文章がわかりにくいので修正してみました。別紙をご覧ください。 【別紙内容】 電子署名法上、証明書の一時停止、一時停止解除について規制している条項はありませんので、一時停止及び一時停止解除の実施は妨げられません。実際には、認定認証事業者が運用規程（CP/CPS）において、「本認証局は、証明書の一時停止は行わない」ことを規定しているものがほとんどです。すなわち、適切な運用規程を設けることで、証明書の一時停止、一時停止解除を取り扱うことは可能だと考えます。
Q2	状況説明の部分を A から Q に移すべきです。別紙をご覧ください。 【別紙内容】 Q: 会員組織で運営されており、当該組織会員のみを利用対象者としている認証局において、会員個人が会員組織から脱退した場合や会員資格を失った場合の、会員組織からの申請による電子証明書の一時停止・一時停止解除を導入することは可能でしょうか？ A: 予め運用規程（CP/CPS）や利用者規約等で規定しておけば、問題ないと考えます。「電子証明書一時停止」の扱いにつきましては、Q1 の回答を参考にしてください。 なお、「電子証明書の一時停止」の導入に関しましては、運用条件や、署名検証者側のシステム対応状況等についても十分ご確認の上、慎重に進めてください。
７．業務体制	
ご意見	
Q1	「最小限の員数あるいは兼務等で業務を実施できるように運用体制を変更する場合」とはどういう意味でしょうか。説明を補ってください。
Q2	変更申請不要という意味でしょうか。それとも，A2 記載の条件を守っているのであれば申請不要だがそうでなければ必要，という意味でしょうか。結論を明確にしてください。

8 鍵更新	
ご意見	
Q1	文章がわかりにくいので修正してみました。別紙をご覧ください。 【別紙内容】 鍵更新調査時に指定調査機関の立ち会いの下で生成作成した新しい発行者署名符号、発行者電子証明書及びリンク証明書ペアについては､変更認定の取得を以て使用可能となります。変更認定の取得までの間は、誤った使用の防止を含め安全に保存される必要があります。従って、新しい発行者電子証明書の外部への提供にあっては、変更認定の取得後に実施頂くことが望ましいものと考えます。 また、機能検証用に使用する利用者の電子証明書についても、新しい発行者署名符号に更新した認証業務から正規に発行された利用者の電子証明書を提供して検証を実施していただく必要があります。この場合、正規に発行された利用者の電子証明書は、まさに正規の電子証明書ですので、その取扱は、認証業務の運用規程（CP/CPS）に則って行われる必要がある点に、注意してください。 なお、以下の点については、遵守いただく必要があります。 ① 鍵更新に係る変更調査の場合も、通常の変更調査と同様、調査完了後は、調査実施前の状態で運用を継続し、認定を取得後に、当該変更を実施できることとなります。すなわち、鍵更新に係る変更認定を取得するまでは、旧鍵での運用を行う必要があり、認定を取得するまでの期間は、調査時に作成した発行者署名符号、発行者署名検証符号(発行者電子証明書)及びリンク証明書は、公開を含め使用することができないと解されます。従って、本件の場合も、認定を取得するまでは、新鍵に係る発行者電子証明書を検証システム側に提供することはできません。 ② 変更調査時に作成したテスト用利用者証明書は、機能試験以外での利用は、認められませんので、調査完了前に全て失効されている必要があります。
Q2	
9．業務廃止	
ご意見	
Q1	留意点の(1)について，「全ての事前調整終了後、社内決定し」が 3 回くりかえされているので最初にまとめるべきです。別紙をご覧ください。 他にも何箇所か文言を修正しました。 【別紙内容】 業務廃止時の留意点 （1） 業務廃止の周知 全ての事前調整終了後、社内決定し、以下の措置をとってください。

・速やかに主務大臣へ書面により届出を提出してください。主務省への廃止届けのコピーを指定調査機関にも提出をお願いします。

・利用者へ書面により周知を行って下さい。

・リポジトリ（Web 等）により社外へ公表して下さい。

（２） 利用者への業務廃止周知後の問合せ対応

・更新利用を予定している利用者へ推奨事業者を提案して下さい。

・現在の利用者に不安を与えない説明を準備して下さい。

・対応者による説明の差異をなくすためのマニュアルを準備して下さい。

（３） 失効処理、CRL/ARL 等

・自己署名証明書(新及び旧自己署名証明書)は、失効しないで下さい。失効してしまうと、その後の検証ができなくなります。

・業務廃止に伴う失効時にも、利用者へ失効完了通知書を送付して下さい。

・最後の CRL/ARL の nextUpdate は、当該最終 CRL/ARL の公開を終了する日よりも先の日にして下さい。これは、公開中に、nextUpdate を過ぎると、無効な CRL/ARL と判断されてしまうためです。

・自己署名証明書(新及び旧自己署名証明書)については、最後の CRL/ARL の公開中は、現在と同様に掲載して下さい。

・フィンガープリントについては、最後の CRL/ARL の公開中は、現在と同様の改ざん防止措置を維持した状態で公開して下さい。

（４） 帳簿書類の保存

・適切な保存措置（漏えい、滅失又はき損防止措置）を施して保存すること。

・1 年保存の帳簿書類については、保存は 1 年でよく、廃棄時に廃棄の記録を残してください。

・10 年保存の要件が課せられているもの(申込書類、規程類等)については、業務廃止後も施行規則第十二条第二項に基づき、引き続き保存するようにしてください。

・利用者電子証明書、自己署名証明書、リンク証明書、相互認証証明書及び CRL/ARL 等を、電子データで保存する場合は、CD,DVD あるいは、DAT 等長期保存が可能で、読み出しに特別なソフトウェアを必要としないと思われる媒体で保存してください。

（５） その他

・電子証明書発行受付終了日が決定したときは、その旨を CP、CPS 等の規程類に記載すること。

・指針第十四条第四号に基づき、発行者署名符号（複製されたものを含む）について完全に廃棄すること。

１０．その他

１０．１　プロファイル

ご意見

Q1	質問文が，一文で長いので二文に分けました。別紙をご覧ください。他にも文言を修正しました。 【別紙内容】 Q：認証業務で使用している組織名として英語表記の略称を使用しております。組織名の英語表記（フルネーム）に変更しても、運用規程（CP/CPS）における組織名の定義を変更することで、継続して使用したいと考えておりますが、変更認定の申請が必要でしょうか？ A：電子証明書に記録しなくてはならない事項として、施行規則第六条第五号のイに「当該電子証明書の発行者の名称」が規定されています。したがって、組織名の英語表記としては、正式な根拠のある英語表記を電子証明書に記録すべきであると思料いたします。 貴認証局の現行の組織名は、組織名の英語表記（フルネーム）の略称を組織の意思決定機関の承認を受けて使用しており、英語表記（フルネーム）の変更後も“xxxxxxx”が組織名称の「呼称」であることを組織の意志決定機関にて正式に承認した上で、運用規程（CP/CPS）に定義するのであれば､引き続き電子証明書の issuer 及び subject に記載する組織名(organizationalName)として“xxxxxxx”を使用することは、認定基準に適合するものと思料いたします。 また、貴認証局の英語表記についても、組織名の英語表記（フルネーム）を変更した後も、現行のままで変更しないことを組織の意思決定機関にて正式に承認するのであれば､引き続き電子証明書の issuer 及び subject に記載する組織単位名(organizationalUnitName)として“xxxxxxxxxxxxxxxxxxCA”を使用することは、認定基準に適合するものと思料いたします。 変更認定の要否につきましては、今回のお問合せによる変更箇所が、運用規程（CP/CPS）で定義している組織名の「略称」を「呼称」とするだけであることから、電子署名法第四条第二項第三号の事項の変更には該当せず､変更認定の必要はないと思料いたします｡実施に際しましては、変更に伴う規程改訂等の記録を残してください。次回更新調査時に、指定調査機関による実地調査を受けていただきますようお願いいたします。
Q2-1	規則 6 条 8 号を参照するのであれば，誤認を避けるための措置に言及すべきです。別紙のように文章を補ってみました。 【別紙内容】 利用者証明書に記載されている利用者の氏名を除く属性情報（事務所所在地の都道府県、市区町村以下等）の証明を空白とすることは可能です。 利用者証明書が、「属性情報（事務所所在地の都道府県、市区町村以下）が記載されたもの」と「属性情報（事務所所在地の都道府県、市区町村以下）が空白のもの」の２種類が併存することになりますので、運用規程（CP/CPS）他関連規程に、次のことを明記してください。 a. 属性情報（事務所所在地の都道府県、市区町村以下）を、空白とした新たな利用者証明書への切り替え時期を明確にすること b. それ以前に発行された利用者証明書（属性情報（事務所所在地の都道府県、市区町村以下）が記載されているもの）は引き続き有効とするのであれば、以前の運用方式を継続（利用者証明書に記載された、いずれの属性情報が変更になっても失効させる）すること c. 利用者証明書のプロファイル等の記述は、２種類のものを併記する、及びその適用時期を

	明確にすること なお、当該変更の前後を通じて、事業所所在地等の属性情報が、認定認証業務に係るものであると誤認されることがないように、適切な措置をとる必要があります。
Q2-2	ご参考願います→ご参照願います
Q3	
１０．２　リポジトリ	
Ｑ１	関係法令は，法４条２項３号ではないでしょうか。
Ｑ２	同じ内容が二回くりかえされています。
Q3	「ご提示いただきましたホームページの変更案」を知らない人を前提に，記載すべきです。
１０．３業務運用者用電子証明書	
Ｑ１	「プロダクト」とは何でしょうか。ソフトウエアかハードウエアか，など説明を入れてください。
Ｑ２	
１０．４　認証事業者による利用者署名符号の生成措置	
Ｑ１	文章がわかりにくいので修正してみました。別紙をご覧ください。 【別紙内容】 本件変更は、変更認定を取得する必要はないものと思料します。 IC カード等を利用者に安全に送付するため、送付手段として本人限定受取郵便（特例型）による場合には、郵便引受番号が記録された受領証（紙）を電子化して安全な保管措置をとってください。これらは、本人限定受取郵便（特例型）を使用した証拠として利用できますし、郵便事故等の際に送付物の追跡を容易にするためにも必要です。また、S/MIME を使用して送付する場合には、暗号化するとともに、電子署名を付した形での通知を行って頂ければと考えます。 なお、送信に使用する電子証明書は認定認証業務で発行されたものが望ましいと考えます。非認定認証業務から発行される電子証明書を用いる場合は、当該電子証明書の仕様もあわせてご提示下さい。
Ｑ２	文章がわかりにくいので修正してみました。別紙をご覧ください。 【別紙内容】 PIN の生成の方法や発送方法に変更は無く、規程にも変更が無い程度の変更であれば、「電子証明書発行チェックリスト」の変更を伴う自動封入封かん機への用紙のセットや精製水の確認等のチェック項目があったとしても、変更認定の申請は必要ありません。
Q1-1	文章がわかりにくいので修正してみました。別紙をご覧ください。 【別紙内容】 利用者署名符号のような電磁的記録媒体のみを単体で送付する場合には、信書の送達にはあたらないと思料します。 しかしながら、業務上利用者署名符号のみを単体で送付することは通常では想定できません。利用者という特定の受取人に差し出す趣旨が明かな文言が記載されている文書を電子的

	記録媒体と共に同梱した場合には、郵便法及び信書便法に規定された「信書」に該当することが想定されます。判断に迷うようなケースでは、総務省が定めた「信書に該当する文書に関する指針」及び「「信書に該当する文書に関する指針(案)」に対する意見の概要」等と総務省の考え方を参考にしていただき、さらにご不明な点は送付内容を判断し、必要に応じて総合通信局または総務省（情報流通行政局郵政行政部郵便課）にお問合せいただければと考えます。
Q1-2	
Q1-3	
１０..５　その他	
Q1	Q の「公的認証サービス」を「公的個人認証サービス」に修正しました。 A の最後の文書に「公的個人認証サービス都道府県協議会にお問い合わせください。」

全体に対して

ご意見

4.1.5 4.2.5 認定認証事業者からの問い合わせ Q&A（帳簿書類の保存場所編）

(諮問委員からのご意見)

a） 手塚委員

１．新規の帳簿保管場所

	ご意見
Q1	特に問題なし。
Q2	特に問題なし。

２．認定済の帳簿保管場所について

	ご意見
Q1	特に問題なし。
Q2	特に問題なし。
Q3	特に問題なし。
Q4	「もし、定期的に帳簿書類を移動するような場合については、移動に関する規定を作成し、移動の実施を記録する帳簿を作成し、実施するようにして下さい。」と書かれていますが、定期的でなくても、異動の実施を記録する帳簿を作成する必要があると考えます。

３．帳簿の媒体変更について

	ご意見
Q1	特に問題なし。
Q2	
Q3	特に問題なし。

４．業務廃止あるいは業務委託終了について

	ご意見
Q1	特に問題なし。
Q2	特に問題なし。

全体に対して

	ご意見
	特に問題なし。

b) 早貸委員

１．新規の帳簿保管場所

	ご意見
Q1	
Q2	

２．認定済の帳簿保管場所について

	ご意見
Q1	
Q2	
Q3	
Q4	「保存義務がある帳簿が委託先で保管して いる場合」 →　保存義務がある帳簿が委託先で保管されている場合 or　保存義務がある帳簿を委託先で保管している場合 のどちらかに修正するほうがよいと思います。

３．帳簿の媒体変更について

	ご意見
Q1	
Q2	
Q3	

４．業務廃止あるいは業務委託終了について

	ご意見
Q1	
Q2	

全体に対して

	ご意見

c) 宮内委員

１．新規の帳簿保管場所

	ご意見
Q1	関連法令をどこまで書くのか，やや難しいと思っています。 設備に関する変更認定は，法 9 条 1 項(及び法 4 条 2 項 2 号)により変更認定が必要となるとともに，法 9 条 3 項により法 6 条 1 項 2 号が準用されて，変更認定の申請に関する規則 6 条 15 号へが適用される，ということだと思います。この事情を全て書くのは無理かもしれませんが，規則 6 条 15 号へだけを記載しても，分かりにくいのではないかと思います。ここは，工夫が必要と思います。
Q2	「規則 6 条 15 号へ」は，「同時に実施できる」根拠とはいいにくいので，関連法令は外してもよいのではないでしょうか。

２．認定済の帳簿保管場所について

	ご意見
Q1	内容は正しいと思います。「保管場所を認定対象外とする」の意味は「複数ある保管場所の一部を認定対象から外す／保管場所とするのをやめる」ということですね。今の文章は，あたかも，保管場所がなくなるような印象を受けるので，若干，文章を調整していただきたいと思います。 なお，関連法令は外してもよいと思います。
Q2	関連法令は，法 9 条 1 項本文，又は，法 9 条 1 項但書き＋規則 9 条だと思います。
Q3	同上
Q4	同上

３．帳簿の媒体変更について

	ご意見
Q1	内容には問題がありません。 ２行目：「又は」→「又は」とすべきです。
Q2	関連法令は，法 9 条 1 項本文，又は，法 9 条 1 項但書き＋規則 9 条だと思います。
Q3	内容的には問題ありません。 以下は，本問の内容とは直接関係しませんので，A3 を変更する必要はありません。 新設分割によって設立される会社が契約上の地位を継承するのに，契約相手の了承は不要です(相手方は債権者として異議を申し立てることは可能です(会社法 810 条参照）)。したがって，新設分割の場合に（原契約を解除して)新設会社との契約を結びなおすとは限らないと考えます。

４．業務廃止あるいは業務委託終了について

	ご意見
Q1	特に問題ありません。

Q2	状況の設定が，やや分かりにくいと感じます。委託先で帳簿書類を管理していて，委託を終了する場合，普通は帳簿書類を委託元に戻すと考えます(その上で，新しい委託先に管理させる等の処理をとりそう)。旧委託先で管理を継続することは，考えにくいのではないでしょうか。 この点を踏まえて，ここで言うべき内容を考えますと，以下のとおりとなり，この順序で書くべきだと思います（文面はお任せします)。 ①帳簿書類は 10 年間の保存義務があるので，どこで管理していようとも，廃棄はできない。 ②委託が終わったら普通は委託元に戻すだろう。その場合には，更新調査時の保管状況の確認は委託元で行う(委託先には行かない)。 ③何らかの事情で(旧)委託先での管理を続ける場合には，更新調査時に(旧)委託先の保管状況を確認することになる。 それから，委託契約書について記載するのは蛇足に見えます。これを書く必要があるのでしたら，別の Q を設けるべきだと思います。
全体に対して	
	ご意見
	特にありません。

4.3 実務者説明会

別冊 1 平成 23 年度(2012)実務者説明会資料を外部有識者に送付し、各諮問委員の方から以下のようなご意見を頂いた。

(諮問委員からのご意見)

a) 手塚委員

１．変更認定について

１．１変更認定の事例集（一覧）

ご意見
「今回新たに整理・追加した事例」の赤枠があるが、これについて後の説明に特記がないのが気になるので、何らかの説明がある方が良いと思います。

１．2　変更認定の事例集（補足説明）

ご意見
特になし。

１．3　変更認定に該当しなかった事例集（一覧）

ご意見
特になし。

１．4　変更認定に該当しなかった事例集（補足説明）

ご意見
特になし。
２．実運用上から見た業務遂行時の留意点等
２．1　実運用上から見た業務遂行の留意点等
ご意見
特になし。
２．２　指定調査機関からのお願い
ご意見
特になし。
３．電子証明書格納媒体
３．１　東日本大震災から見えたこと
ご意見
本件のまとめをしたことは非常に良いことで、実務者で情報を共有することは大変有用であると思います。
３．２　激甚災害時における対応
ご意見

特になし。
４．暗号アルゴリズム SHA-1 および RSA1024 に係る移行に関する広報について
ご意見
緊急時対応計画との関係に言及することも必要であると考えます。

全体に対して

ご意見
「実務者説明会」は大変重要な会議であり、我が国における電子署名法の健全な発展に寄与するものであると考えます。 今後も定期的に開催をしていただきたいと思います。

(b) 早貸委員

１．変更認定について

１．１変更認定の事例集（一覧）

ご意見
P4 中の「基本的には、「同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設」以外は、すべて変更認定。」の部分については、「認定基準に関わる要素の変更については」との前提が必要かと思います。当たり前のことなので、省略されているかとは思いますが。

１．２　変更認定の事例集（補足説明）

ご意見

１．３　変更認定に該当しなかった事例集（一覧）

ご意見

１．４　変更認定に該当しなかった事例集（補足説明）

ご意見

２．実運用上から見た業務遂行時の留意点等

２．１　実運用上から見た業務遂行の留意点等

ご意見
８８P　「統一的に実施」については、「整合性が取れるように実施」の意味ですかね。

２．２　指定調査機関からのお願い

ご意見

３．激甚災害時の対応について

３．１　東日本大震災から見えたこと

ご意見

３．２　激甚災害時における対応

ご意見

４．暗号アルゴリズム SHA-1 および RSA1024 に係る移行に関する広報について

ご意見

全体に対して

ご意見

c) 宮内委員

１．変更認定について

１．１変更認定の事例集（一覧）

ご意見
特にありません。

１．2　変更認定の事例集（補足説明）

ご意見
p.14 について。規則 9 条により変更認定対象外となる余地はないのでしょうか。 P.22 について。各「・」末尾の「の調査」は不要です。（本文で「以下の措置状況」と言っている） p.34 について。タイトルは「……利用申込み方法の追加」とする方がよいでしょう。 p.36 について。タイトルは「……保存方法の変更」とする方がよいでしょう。

１．3　変更認定に該当しなかった事例集（一覧）

ご意見
特にありません。

１．4　変更認定に該当しなかった事例集（補足説明）

ご意見
特にありません。
２．実運用上から見た業務遂行時の留意点等 ２．1　実運用上から見た業務遂行の留意点等
ご意見
特にありません。
２．２　指定調査機関からのお願い
ご意見
特にありません。
３．激甚災害時の対応について ３．１　東日本大震災から見えたこと
ご意見
特にありません。
３．２　激甚災害時における対応
ご意見
特にありません。
４．暗号アルゴリズム SHA-1 および RSA1024 に係る移行に関する広報について

ご意見
特にありません。

全体に対して

ご意見

平成 24 年 3 月発行

発行所　一般財団法人日本情報経済社会推進協会
東京都港区六本木一丁目９番９号
六本木ファーストビル内
ＴＥＬ　03（5860）7571