

平成27年度(2016年) 実務者説明会(説明会資料抜粋)



日時:平成28年3月3日(木) 14時～16時

場所:六本木ファーストビル1階(第1～3会議室)

(東京都港区六本木1-9-9)

一般財団法人日本情報経済社会推進協会

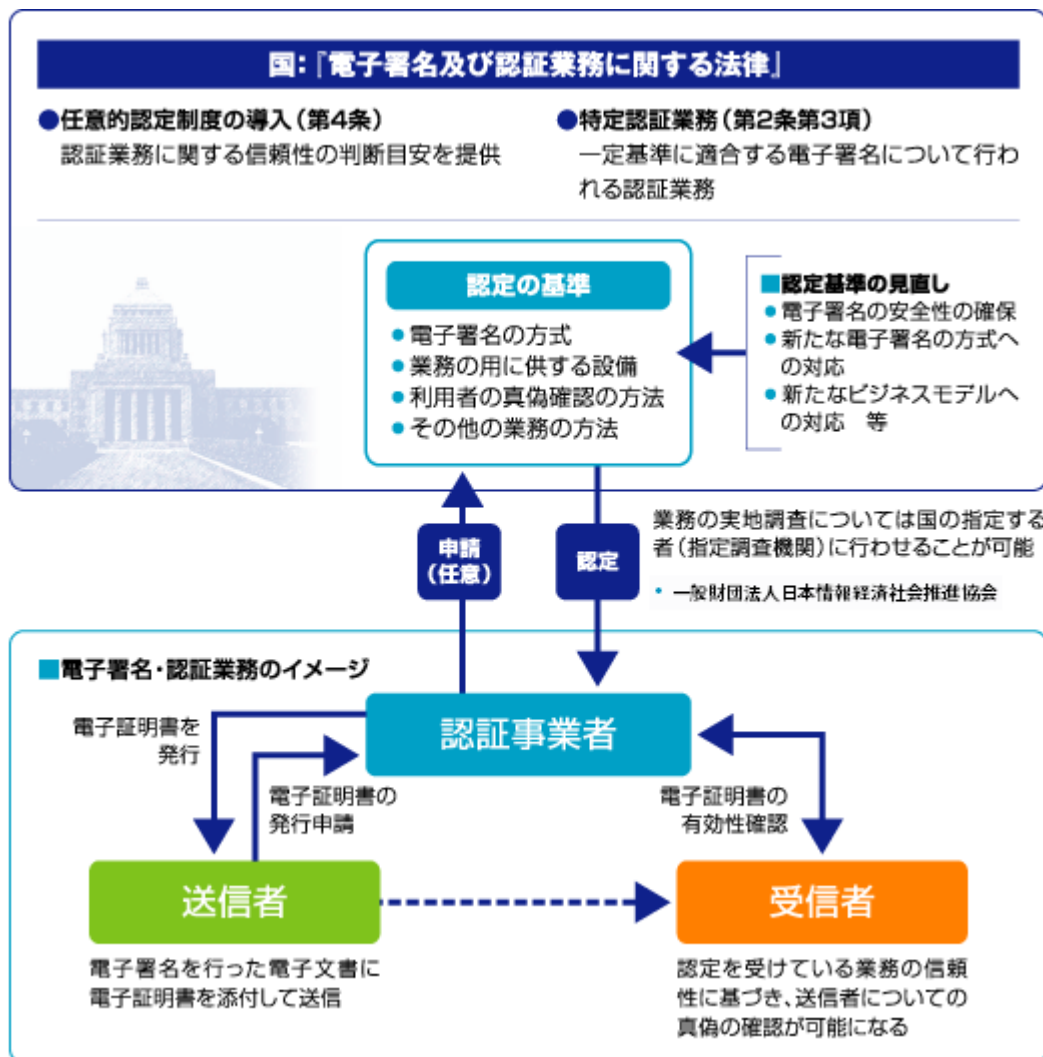
電子署名・認証センター

目次

1. 電子署名法と変更認定
2. 真偽確認に関するトピックス
3. 電子署名法研究会の状況
4. 施行規則の改正について

1. 電子署名法と変更認定

法第3条の「電磁的記録の真正な成立の推定」を支える
特定認証業務に関する認定の制度



特定認証業務の認定を受けるためには、どのような技術・設備水準が必要なのか示されており、電子署名の方式や業務の用に供する設備、利用者の真偽確認の方法等が定められ、こうした認定を受けた認証局が発行する電子証明書は、一定レベルの信頼性を保ったものだと判断される。

1. 電子署名法と変更認定

(1) 認定の基準に関する電子署名法令等の条文

法第四条(認定)

特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

2 前項の認定を受けようとする者は、主務省令で定めるところにより、次の事項を記載した申請書その他主務省令で定める書類を主務大臣に提出しなければならない。

- 一 氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
- 二 申請に係る業務の用に供する設備の概要
- 三 申請に係る業務の実施の方法

法第六条(認定の基準)

主務大臣は、第四条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。

- 一 申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。
- 二 申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること。
- 三 前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。

<凡例(スライド3及び4)> ○真偽確認方法・マゼンタで記載
○設備の要件・青字で記載 ○業務の方法・緑字で記載

1. 電子署名法と変更認定

(業務の用に供する設備の基準)

施行規則第四条 法第六条第一項第一号の主務省令で定める基準は、次のとおりとする。

第一号～第五号(調査表1100～1500)

(利用者の真偽の確認の方法)

施行規則第五条 法第六条第一項第二号の主務省令で定める方法は、次の各号に掲げる方法とする。

第一項～第二項(調査表2100～2200)

(その他の業務の方法)

施行規則第六条 法第六条第一項第三号の主務省令で定める基準は、次のとおりとする。

第一号～第十七号(調査表3100～3E00)

※ 解説

法第六条で定められた「認定の基準」は、さらに施行規則や指針・方針に落ちてきて、より具体的で細かな判断基準が定められ、事業者が実施している業務一つ一つに展開されている。

1. 電子署名法と変更認定

(2) 変更認定に関する電子署名法令等の条文

法第九条(変更の認定等)

認定認証事業者は、**第四条第二項第二号又は第三号**の事項を変更しようとするときは、主務大臣の認定を受けなければならない。
ただし、主務省令で定める**軽微な変更**については、この限りでない。

施行規則第九条

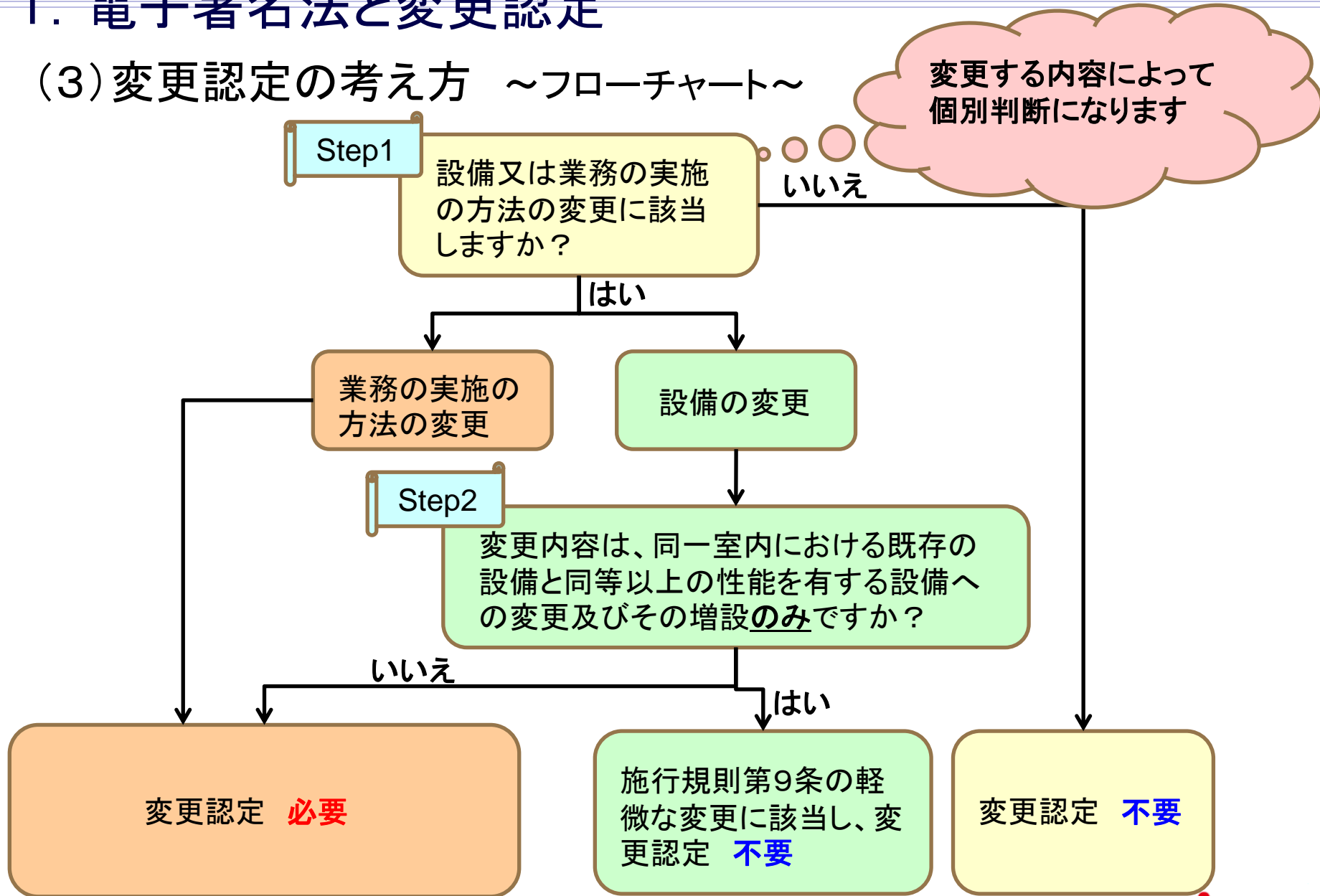
法第九条第一項ただし書の主務省令で定める軽微な変更は、**同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設**とする。

※ 解説

法第四条で定められた「認定」の申請に関する事項の変更に該当すると判断された場合は、変更認定が必要である。

1. 電子署名法と変更認定

(3) 変更認定の考え方 ~フローチャート~



1. 電子署名法と変更認定

(4) 変更認定を**必要**とした事例

※ 昨年の説明会開催以降、該当する事例なし

(5) 変更認定を**不要**とした事例

昨年の説明会開催以降、主務三省及び指定調査機関に問合せがあり、変更認定は不要であると判断された事例を紹介する。

個々の事業者が特定されずかつ汎用的に参考になると考えられる事例を抽出

<設備系>

- ① 認証業務用設備の通信プロトコルの変更
- ② 空調設備及び照明設備のリプレース
- ③ 認証業務用設備に対するWindows10対応用のパッチ適用

<業務系>

- ④ 利用者証明書のプロフィール変更(CRLDPのURLの変更)
- ⑤ 利用申込書・失効関連書類の外部保管
- ⑥ オペレータ用証明書の暗号アルゴリズム変更
- ⑦ 電子証明書に付加する資格属性情報の削除
- ⑧ 有効期間の長い利用者証明書発行および再発行の対応変更

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

<凡例>

○法・・・電子署名法

○施行規則・・・電子署名法施行規則

① 利用者識別符号等受信設備に対する通信プロトコルの変更

(質問)

メンテナンス用PCから利用者識別符号等受信設備への通信手段としてtelnetやftpを利用してアクセスしていたが、当該設備更改にあたり、通信プロトコルをtelnetはsshに、ftpはscpに変更する。

本プロトコルの変更による運用への影響はないため、軽微な変更であると認識しているが、念のため確認したい。

(回答)

変更認定は不要である。

メンテナンス用PCから当該設備への通信手段の変更は、法第4条第2項第2号に規定する設備の概要の変更には該当せず、法の対象外であるため。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

② 空調設備及び照明設備のリプレイス

(質問)

入居しているビルの空調設備(登録用端末設備室)及び照明設備(登録用端末設備室・認証設備室)が老朽化のためにリプレイスされるが、この変更は軽微な変更としてよいか。

なお、リプレイスする設備一式については、機能面での向上が見込めるものであり、劣化することはない。

(回答)

変更認定は不要である。

空調設備(登録用端末設備室)及び照明設備(登録用端末設備室・認証設備室)の変更は、法第4条第2項第2号に規定する設備の概要の変更には該当せず、法の対象外であるため。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

③ 認証業務用設備に対するWindows10対応用のパッチ適用

(質問)

先日マイクロソフト社から発売されたWindows10/IE11の組み合わせにおいて、OSの内部バージョン表記が従来の6.xから10.xに変更となったことに伴い、認証業務用設備にパッチの適用を行うことを検討しているが、変更認定は必要であるか。

なお、今回の変更は上記の表記変更に伴うものであり、既存の処理、ならびに署名／暗号処理についての変更はない。

(回答)

変更認定は不要である。

認証業務用設備にパッチを適用することは、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であり、施行規則第9条で定める軽微な変更該当するため。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

④ 利用者証明書のプロフィール変更(CRLDPのURLの変更)

(質問)

EE 証明書・リンク証明書の標準プロフィール(CRLDP)の一部について、アクセス先ドメインの変更が発生するが、変更認定は必要であるか。

(回答)

変更認定は不要である。

利用者電子証明書及びリンク証明書のCRLDP のURL のドメインを変更したとしても、

- ① 施行規則第6条第10号に基づき失効情報をサーバーに記録していること、
- ② 施行規則第6条第11号に基づき失効情報を容易に確認することができるようにすること、

の2点を満たしていることは変わらないため、実態的には業務の運用方法が変わるところはなく、法第4条第2項第3号に規定する業務の実施の方法の変更には該当せず、変更認定は不要と判断する。

ただし、施行規則第6条第10号に規定する「電子証明書に記録された事項に事実と異なるものが発見されたとき」に該当しないように、発行済み利用者電子証明書の有効期限が満了するまで、署名検証者が当該電子証明書の有効性を検証できるよう、変更前ドメインのCRLDPを維持し続ける必要がある。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

⑤ 利用申込書・失効関連書類の外部保管

(質問)

利用申込書等の帳簿書類の一部について外部保管を行う。利用申込書・失効関連書類であり、かつ当該電子証明書が期限切れのものの保管場所を、現在の保管場所から郊外事務所の1室へ変更する。

外部保管にあたり、変更認定の必要性について確認させていただき、懸念点があれば指摘いただきたい。

(回答)

変更認定は不要である。

本件は「保存方法に変更がなく、保管場所のみが変更になる」場合と考えられることから、平成25年度実務者説明会(平成26年2月25日)における説明のとおり、法第4条第2項第3号に規定する業務の実施の方法の変更には該当しないため。

なお、施行規則第12条第1項第1号及び第2号に掲げる帳簿書類の漏洩、滅失等を防止する観点から、負担にならない範囲で、「外部保管する際の手順」を詳細化し関係者間で情報共有を行った上で、実際の作業に際しては作業の記録を残されることが好ましい。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

⑥ オペレータ用証明書の暗号アルゴリズム変更

(質問)

認定認証業務に従事する要員が使用しているオペレータ用電子証明書の暗号アルゴリズムについて、現行アルゴリズム(SHA-1)から新アルゴリズム(SHA-256)での発行となるため、変更認定が必要か確認したい。

(回答)

変更認定は不要である。

オペレータ用電子証明書は、施行規則第4条第2号及び第3号に規定される措置に用いられる設備であるが、暗号アルゴリズムをSHA-1からSHA-256へ変更することは同室内における同等以上の性能を有する設備への変更であり、施行規則第9条で定める軽微な変更に該当するため。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

⑦ 電子証明書に記載している属性情報の削除

(質問)

電子証明書に記載している属性情報の一部を削除し、その属性情報に関する規定内容もすべて削除することとなった場合、変更認定は必要か確認したい。

(回答)

変更認定は不要である。

属性情報の記録は、法で規定された認定認証業務の対象外であるため(施行規則第6条第8号)。

1. 電子署名法と変更認定

(5) 変更認定を不要とした事例

⑧ 有効期間の長い利用者証明書発行および再発行の対応変更

(質問)

有効期間がより長い利用者電子証明書の発行について次の点を確認したい。

質問① 証明書種別の追加

有効期間の長い証明書を追加するにあたって、有効期間が発行日から5年を超えない証明書であれば、変更認定申請の必要はないと考えてよいか。

質問② 既存の証明書種別の一部廃止

既存の証明書種別を一部廃止することは変更認定に該当するか。

(回答)

変更認定は不要である。

個別の証明書の電子証明書種別の追加について電子署名関係法令において規定もないところ、認定を得ている業務のサービスの一環として追加される限り、変更認定の必要はないと考えられる。

なお、有効期間が5年を超える場合、法令違反となることから、そもそも認めることはできないと考えられる(施行規則第6条第4号)。

2. 真偽確認に関するトピックス

本年度は、施行規則が改正されたこと、マイナンバー制度が導入されたことにより真偽確認に関する話題について、特定業務インフォメーションをお送りする機会が多かったです。

また昨年度(平成26年度)の電子署名法研究会において、住民票の写し、印鑑登録証明書等における本人確認方法のルール作りについても提案があり、実際にルールの策定作業が進みました。

ここでは以下の3つの話題について改めて取り上げ、皆さんと情報共有をはかりたいと思います。

- (1) 「在留証明」の真偽確認等について
- (2) 真偽確認ルールの統一化について
- (3) 個人番号記載の住民票の写しの扱い

説明のポイント

昨年9月8日の施行規則改正により、「利用者の真偽の確認」に用いる「主務省令で定める方法」として、「領事館(領事館の職務を行う大使館若しくは公使館の長又はその事務を代理する者を含む。)の在留証明」が明記された。

「在留証明」に関しては、これまでは住民票の写し等に「準ずるもの」として考えられてきたものの、その形式等については周知されておらず、CP/CPS等に「在留証明」を明記されている例もない。

そのため、領事館が発給する「在留証明」の真偽判定に係わる情報等について、外務省領事局領事サービス室に問合せを行い「第6回特定認証業務インフォメーション」として周知したものである。

(1)「在留証明」の真偽確認等について

「在留証明」とは何か？

外国に居住する日本人が当該国のどこに住所(生活の本拠)を有しているかを証明する書類であり、日本の提出先機関から外国における住所証明の提出が求められている場合に発給される証明書。在留の事実(居住の事実)のみが証明される。

以下の2つの書式がある。

- 現住所のみを証明する書式(別添1)
- 過去の住所や同居家族に関する情報を含め現住所を証明する書式(別添2)

(別添1)

在留証明願

形式 1

平成 年 月 日

在スロバキア日本国大使 殿

申請者氏名 証明書を 使う人		生年	(明・大)
		月日	(昭・平)
来訪者氏名 (※1)		申請者との関係 (※1)	
申請者の 本籍地 (※2)	(都・道 府・県)	[市区郡以下を記入してください。 ※2]	
提出理由		提出先	

私(申請者)が現在、下記の住所に在住していることを証明してください。

現 住 所	日 本 語 : スロバキア共和国	
	外 国 語 :	
上記の場所に住所(又は居所)を 定めた年月日(※2)		(平成・昭和) 年 月

(※1) 申請者と同じときは記入不要です。

(※2) 申請理由が恩給、年金受給手続きのとき、及び提出先が同様の記載を必要としないときは記入を省略することができます。

在留証明

証 第 号

上記申請者の在留の事実を証明します。

平成 年 月 日

在スロバキア日本国特命全権大使

江川 明夫

(手数料:)

(1)「在留証明」の真偽確認等について

「在留証明」とは何か？

(別添2)

形式 2

在 留 証 明 願

平成 年 月 日

在アメリカ合衆国日本国特命全權大使
佐々江 賢 一 郎 殿

申請者氏名 証明書を 使う人		生年 月 日	[明・大 昭・平]	年 月 日
来訪者氏名 (※1)		申請者との関係 (※1)		
申請者の 本籍地 (※2)		[都・道 府・県]	(市区町村は下を記入してください。 ※2)	
提出理由		提出先		

私(申請者)が現在、下記の住所に在住していること、及び別紙の事実を証明してください。

現 住 所	アメリカ合衆国	
	日 本 語:	
	外 国 語	
上記の場所に住所(又は居所)を 定めた年月日(※2)		年 月

(※1) 申請者と同一ときは記入不要です。
(※2) 申請理由が更新、年金受給手続などのとき、及び提出先が関係の記載を必要としないときは記入を省略することができます。

在 留 証 明

証 第 BH - 号

上記申請者の在留の事実及び別紙の事実を証明します。

平成 年 月 日

在アメリカ合衆国日本国特命全權大使
佐々江 賢 一 郎

印

(手数料: 米 賃 ドル)

(1/2)

過去の住所

1	年 月 から 年 月 まで
2	年 月 から 年 月 まで
3	年 月 から 年 月 まで
4	年 月 から 年 月 まで
5	年 月 から 年 月 まで

同居家族

1	氏名	生年月日	[明・大 昭・平]	年 月 日
	本籍地	[都・道 府・県]	/	
2	氏名	生年月日	[明・大 昭・平]	年 月 日
	本籍地	[都・道 府・県]	/	
3	氏名	生年月日	[明・大 昭・平]	年 月 日
	本籍地	[都・道 府・県]	/	
4	氏名	生年月日	[明・大 昭・平]	年 月 日
	本籍地	[都・道 府・県]	/	
5	氏名	生年月日	[明・大 昭・平]	年 月 日
	本籍地	[都・道 府・県]	/	

(2/2)

(1)「在留証明」の真偽確認等について

発給条件

- 日本国籍を有する方(二重国籍を含む。)のみ申請ができる。
- 現地にすでに3ヶ月以上滞在し、現在居住していること。ただし、申請時に滞在期間が3ヶ月未満であっても、今後3ヶ月以上の滞在が見込まれる場合には発給の対象となる。
- 証明を必要とする本人が領事館へ出向いて申請することが必要(本人申請が原則)です。ただし、本人が公館に来ることができないやむを得ない事情がある場合は、委任状をもって代理申請される場合もある。
- 領事館で申請する方の意思と提出先機関の確認を行うと同時に、本人の生存確認が行われる。

留意点

- 使用されている用紙は一般的な用紙であり、「透かし」などの偽造防止(複写防止)措置は施されていない。
- 「本籍地」の欄は残されており、在留者本人の旅券に基づいて、本籍地の都道府県名は必ず記入されるが、市区郡以下の住所については、省略されることがある。

(1)「在留証明」の真偽確認等について

証明者と確認方法

- 「在留証明」の証明者は、各国に派遣されている「特命全権大使」又は「総領事」。「特命全権大使」や「総領事」の氏名に関しては、外務省がWebページに公開している「在外公館長名簿」により確認可能。
- 異動等により大使が空席となった場合には、大使館の長の事務を代理する者(臨時大使)が任命され、臨時大使名で在留証明の発給が行われる場合がある。
- 大使が任命されておらず、近隣の大使が「兼轄」している場合には、常駐している大使館の大使名で発給される場合がある。

押印される「公印」

- 約2.3cm角の角印で、「在XX日本国特命全権大使」等と刻印される。
- デザインは統一されおり、書体は篆書体。
- 「在留証明」には、朱印で押印される。

在○◇△□
日本国特命
全権大使

説明のポイント

平成26年度電子署名法研究会において、住民票の写し、印鑑登録証明書等における本人確認方法のルール作りについて、個別具体的なルールテーブルを作成し、メンテナンスしていくことが提案された。そこでまず指定調査機関がすべての認定認証業務における真偽確認状況を取りまとめ、具体的な業務名が判明しない形で表形式に整理し、各業務の了承を得た上で、電子認証局会議殿(CAC)に開示した。CACでは、業務ごとに分かれていた表を一つに取りまとめ、問題点を整理した上で、指定調査機関と主務三省に諮った。その結果、地割以外の取りまとめ結果については、大きな問題はないものとしてひとまず整理されている。

説明のポイント

行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年5月31日法律第27号。以下「番号利用法」という。)において、特定個人情報を提供すること及び収集・保管することは原則として禁止されている。

また、住民基本台帳法(昭和42年7月25日法律第81号)第12条第5項に規定されているとおり、住民票の写しにおいては個人番号の記載を省略することが可能である。

上記の点に配慮し、個人番号が記載された住民票の写しの扱いについて、昨年11月に「第7回特定認証業務インフォメーション」として周知した。

必要な事前の対応

利用者規程や重要事項説明書等に、利用者は申込みの際に個人番号を提供してはならない旨を記載し、利用者に個人番号の記載を省略した住民票の写しを提出していただくよう周知する。

説明のポイント

行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年5月31日法律第27号。以下「番号利用法」という。)において、特定個人情報を提供すること及び収集・保管することは原則として禁止されている。

また、住民基本台帳法(昭和42年7月25日法律第81号)第12条第5項に規定されているとおり、住民票の写しにおいては個人番号の記載を省略することが可能である。

上記の点に配慮し、個人番号が記載された住民票の写しの扱いについて、昨年11月に「第7回特定認証業務インフォメーション」として周知した。

必要な事前の対応

利用者規程や重要事項説明書等に、利用者は申込みの際に個人番号を提供してはならない旨を記載し、利用者に個人番号の記載を省略した住民票の写しを提出していただくよう周知する。

利用者から提出を受けた場合の対応

- ① 事業者において個人番号を「墨塗り」することは、番号利用法に則った行為であるところ、当該行為を行うことについて、事前に利用者に同意を取ることが必須ではないが、施行規則第6条第14号に基づき利用者から開示が求められる場合があるところ、事前に同意を取ることが望ましい(同意の方法については適宜の方法で差し支えない。)
- ② 基本四情報以外の情報(個人番号を含む。)が利用申込者により墨塗りされていた場合については、住民票の原本性が疑われる場合を除き、施行規則第5条第1項第1号の書類として扱って差し支えない。なお、墨塗りされた部分にどのような事項が記載されているか判別できないことなどにより、それが市区町村長の発行したものかどうか不明確な場合は、「原本性が疑われる」と考えられる。
- ③ 個人番号部分が復元できない程度に墨塗りされているのであれば、その方法は問わない。また、番号利用法上、個人番号部分のみを墨塗りすれば足りると思われるところ個人番号項目表示については墨塗りすべきではないと考える。

※上記のほか、番号利用法や「特定個人情報の適正な取扱いに関するガイドライン(事業者編)(平成26年12月11日 特定個人情報保護委員会編)」等に反しない対応が必要

3. 電子署名法研究会の状況

※ 現在開催中の電子署名法研究会配布資料に基づき、次スライドより説明します。

＜平成27年度第1回電子署名法研究会配布資料＞

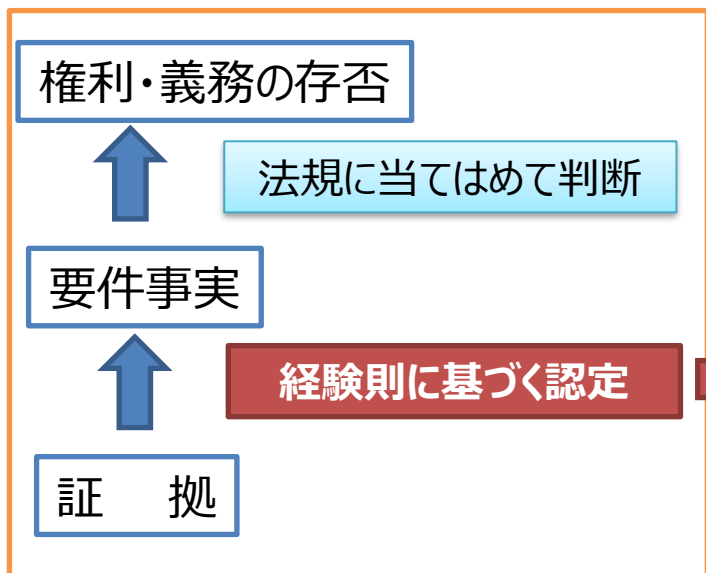
論点整理紙（案）

論点整理紙 (案)

〈議論の評価軸〉 民事訴訟における裁判官の心証形成の程度について

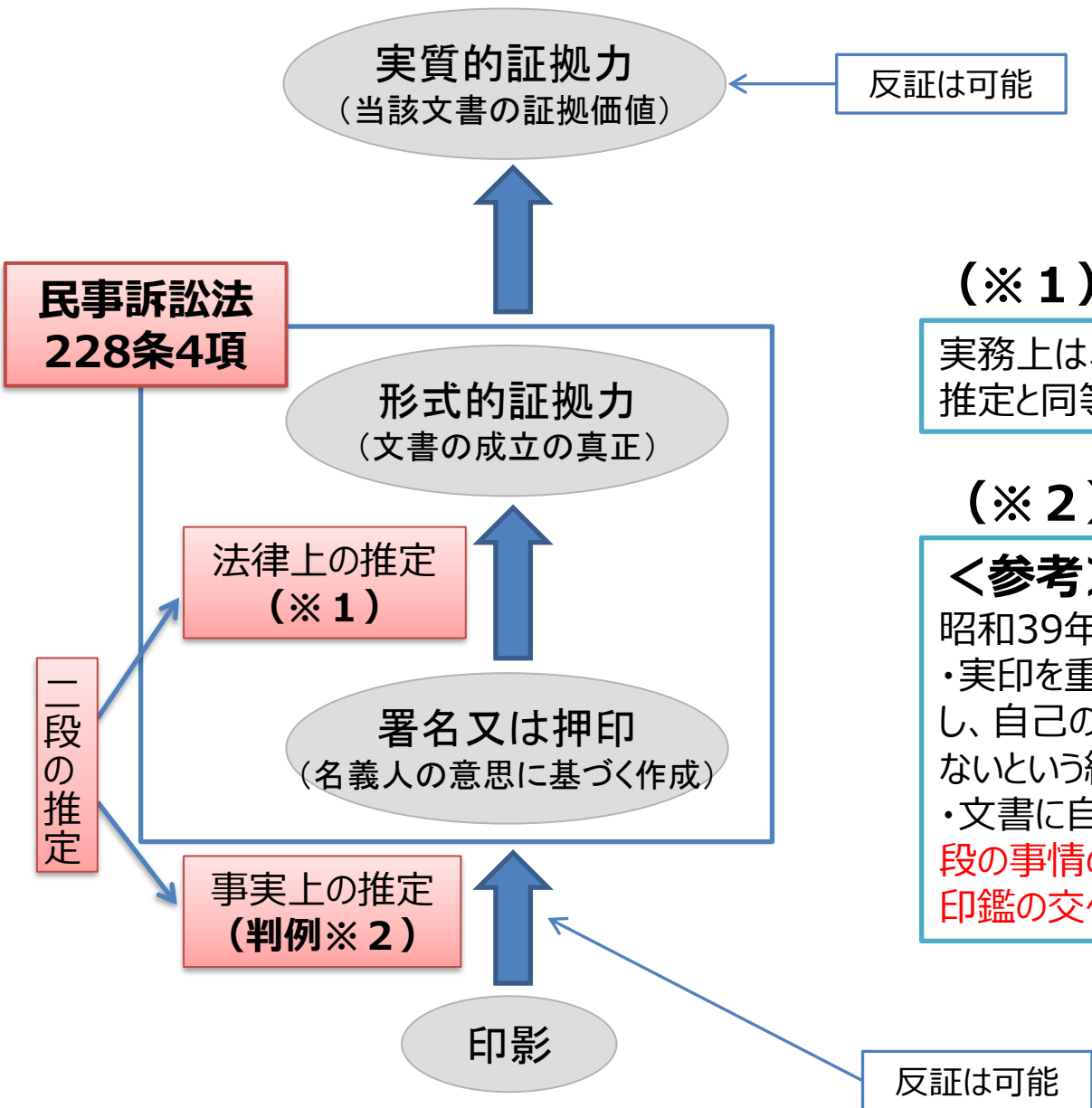
○民事訴訟においては、裁判官が証拠の真正性等を経験則に基づいて認定するところ、心証形成の程度については、以下のとおり、**高度の蓋然性を証明（十中八九確かであるとの判断）**することであるとされている。

民事訴訟におけるプロセス



○**裁判官の心証形成の程度**
（最判昭和50年10月24日参照）

- ・訴訟上の因果関係の立証は、…**高度の蓋然性を証明（十中八九確かであるとの判断）**すること…
- ・その判定は、**通常人が疑を挟まない程度に真実性の確信を持ちうるものであることを要し、かつそれで足りる**



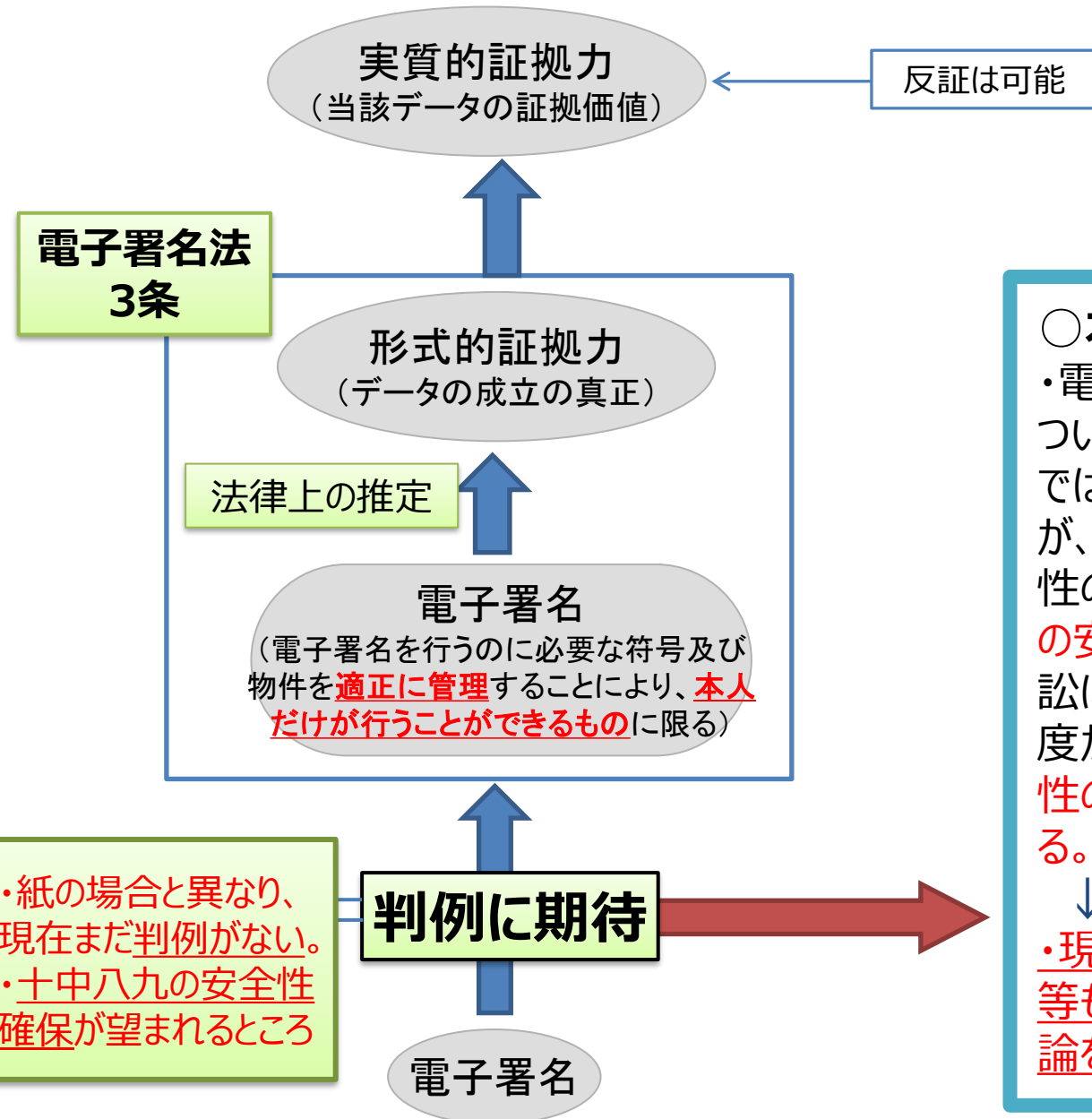
(※1)

実務上は、法定証拠法則、すなわち、事実上の推定と同等の効力を持つものとして扱われている。

(※2)

<参考> 私文書の場合の扱い（最判昭和39年5月12日参照）

- ・実印を重用するわが国の風土・国民気質に照らし、自己の実印をみだりに他人に預託することはないという経験則を基礎として、
- ・文書に自らの実印が押印されている以上は、**特段の事情のない限り、その意思に基づく押印又は印鑑の交付によるものと推認**する。



○ **本研究会のスタンスについて**

- ・電子署名法は、一段目の推定について直接法規で規定しているわけではなく、まだ具体的な判例もないが、認定認証事業が有すべき安全性の基準を考えれば、**サーバ証明の安全性確保についても、民事訴訟における裁判官の心証形成の程度から判断して、十中八九の安全性の確保が望まれるものと考えられる。**
- ↓
- ・現行制度、他システム、国際標準等も比較検討の上、総合的に議論を進めることとしたい。

・紙の場合と異なり、
現在まだ判例がない。
・十中八九の安全性確保が望まれるところ

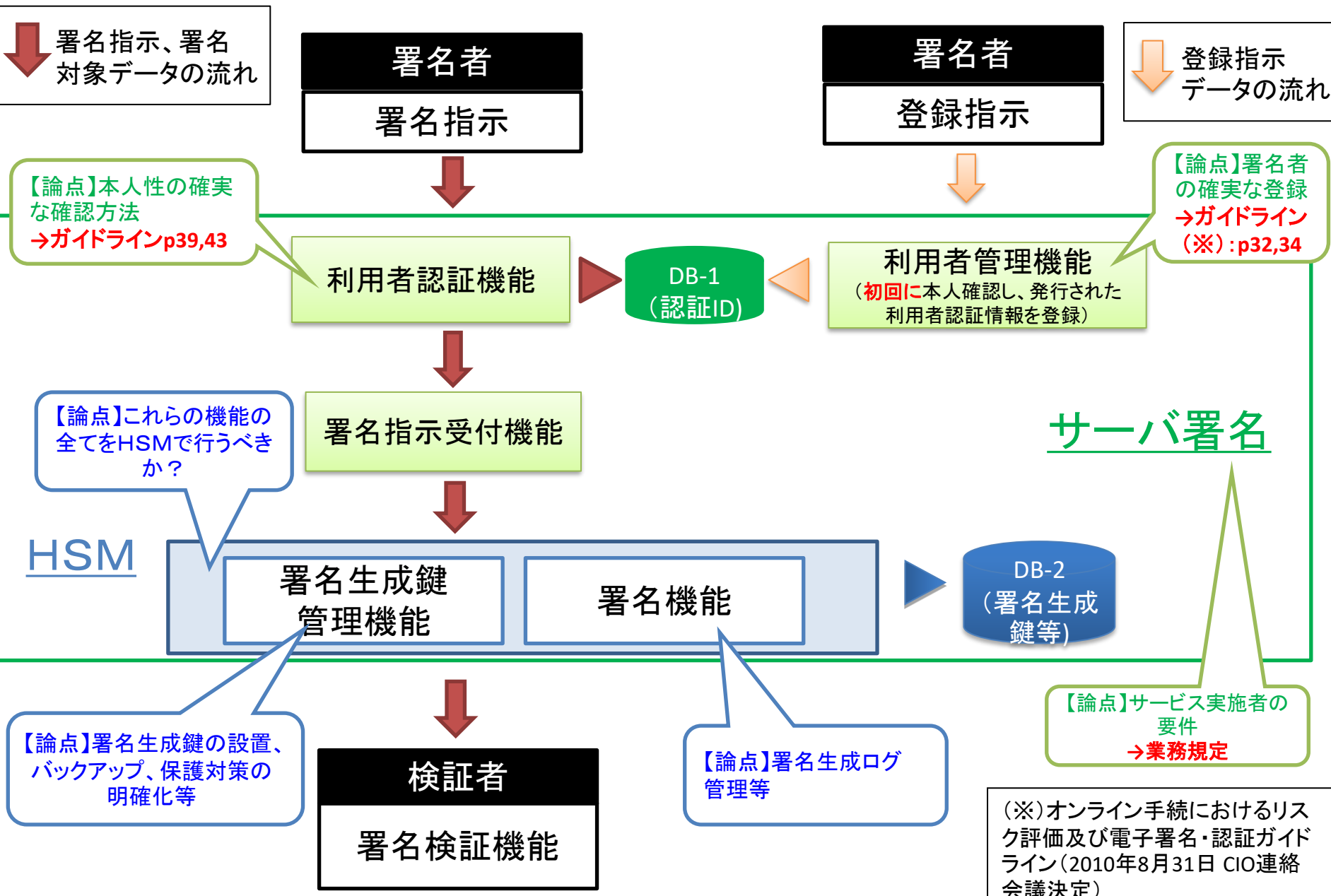
- 1 サーバ署名が導入されると、現行の電子署名の行い方と比べて何がどう変わると考えられるか？
 - ・利便性の高いユースケースにはどのようなものが考えられるか？
 - ・サーバ署名は、日本のサイバーセキュリティ対策の観点からどのようなメリットがあるか？
 - ・安全を担保すべきために規制が必要な業務プロセスや、必要な体制等にはどのようなものが考えられるか？うち、特に必要なものは何か？
- 2 電子署名制度にサーバ署名を導入する場合、以下の改正は必要と考えられるか？
 - ・電子署名法
 - ・同省令、指針等
- 3 規制のレベルはどの程度に設定することが望ましいと考えられるか？

＜平成27年度第2回電子署名法研究会配布資料＞

サーバ署名の機能及び論点

サーバ署名の機能及び論点

資料 1

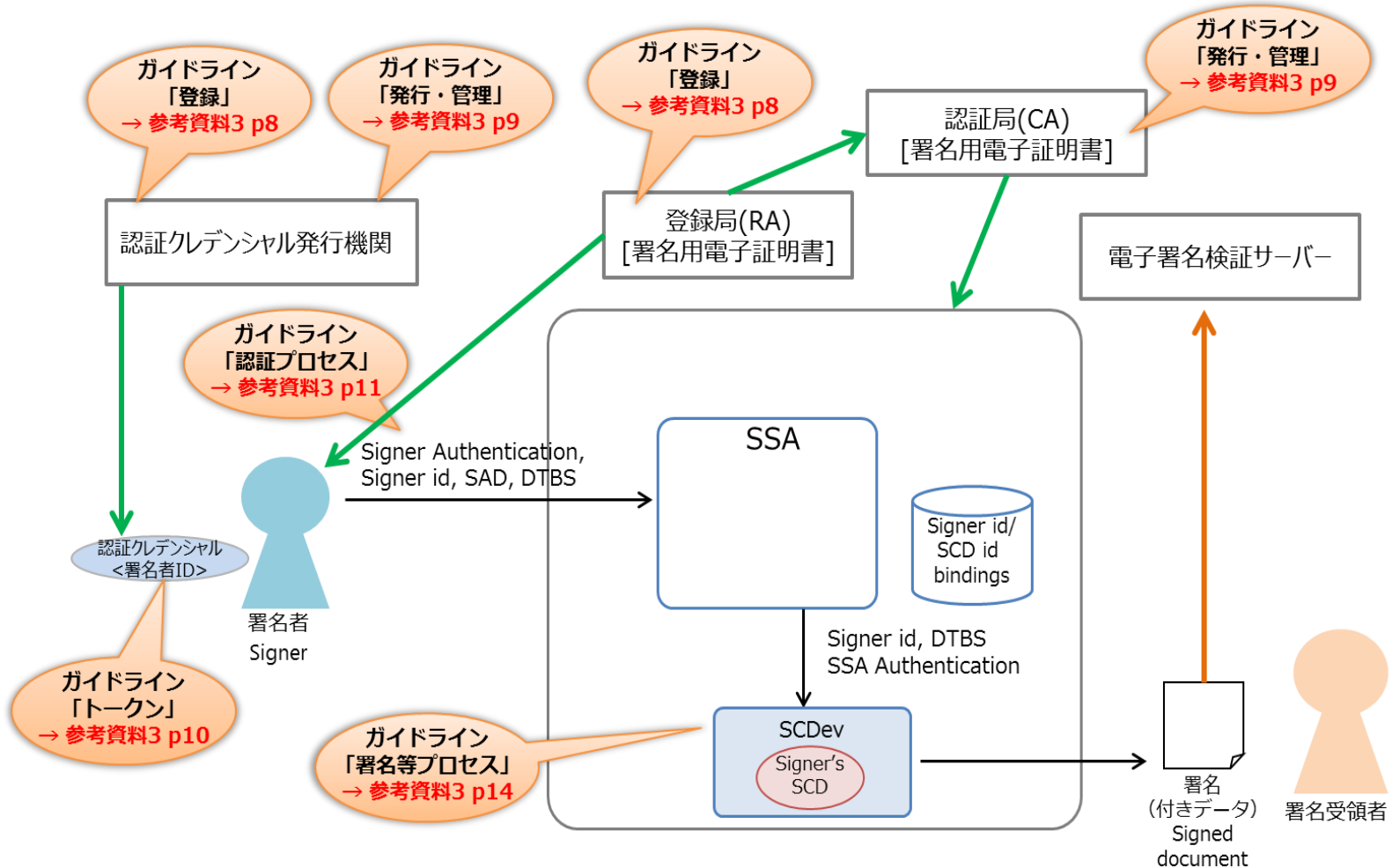


＜平成27年度第2回電子署名法研究会配布資料＞

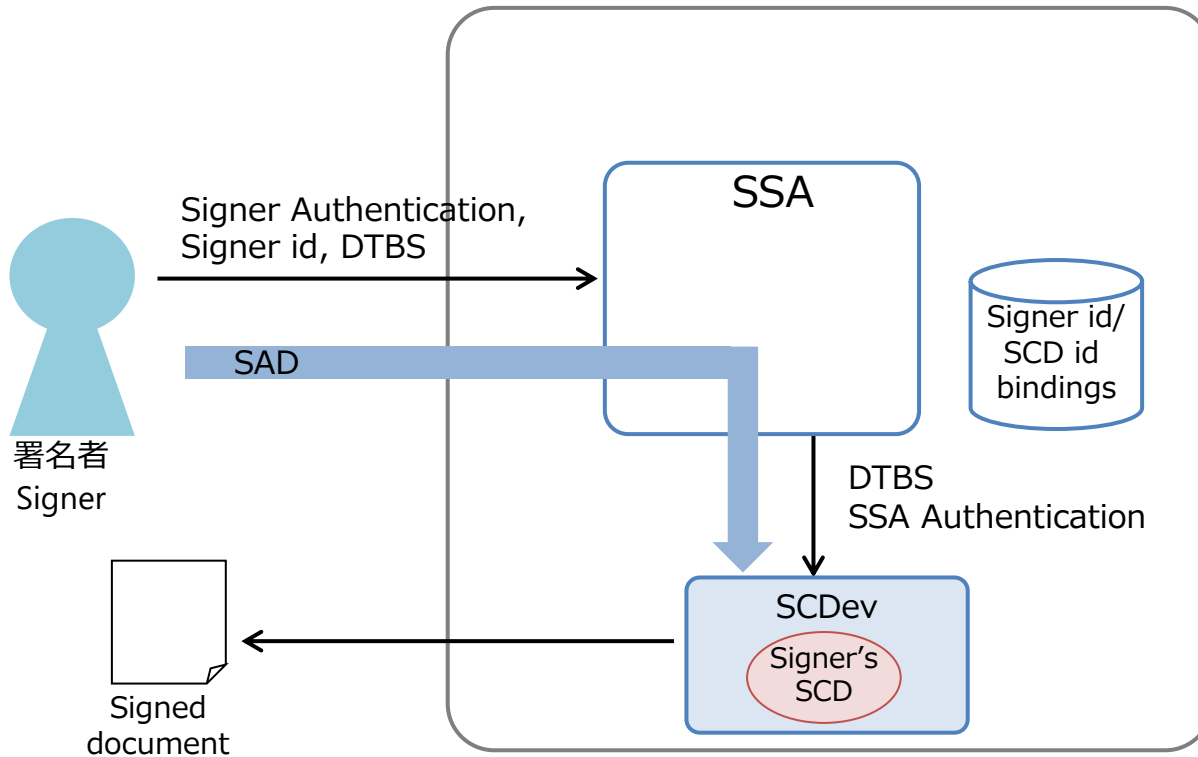
国内サーバ署名事例

1. サーバ署名の国内事例調査について

- インタビュー調査によって確認した国内のサーバ署名の事例を報告する。
- サーバ署名と参考資料3（参照ガイドライン抜粋）との関連を以下に示す。



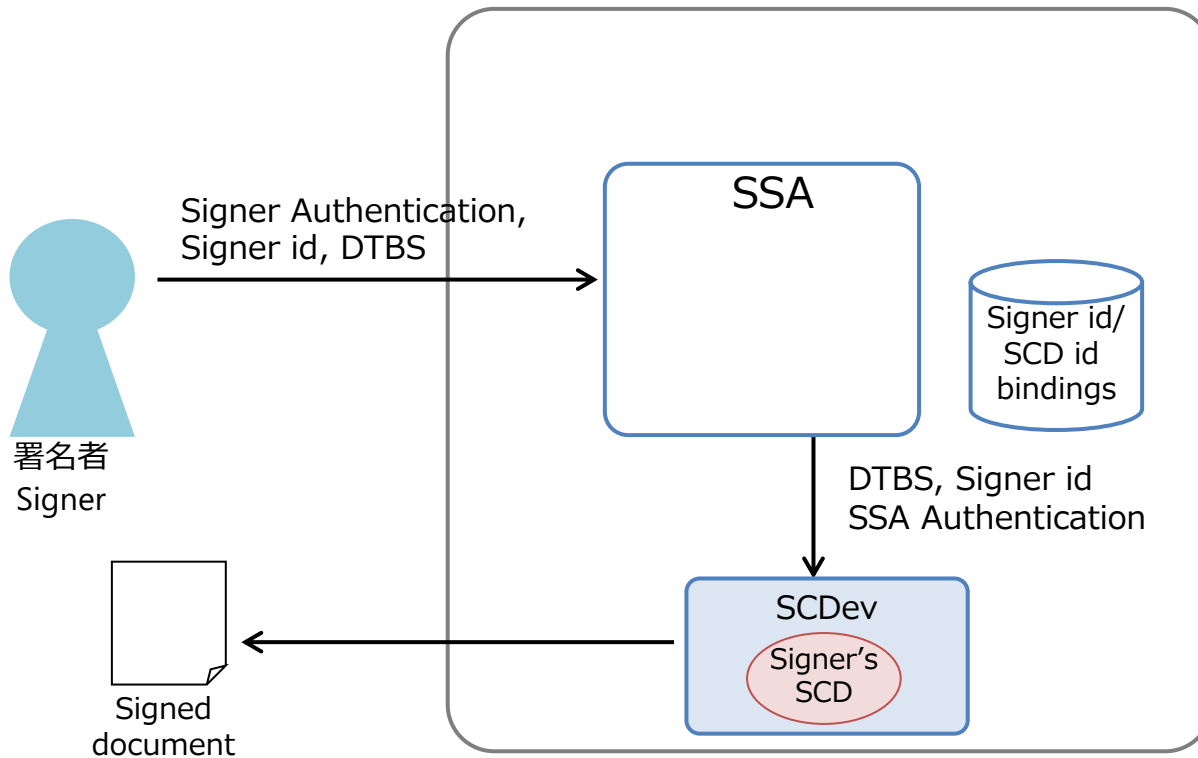
2. 国内サーバ署名事例構成①



■用語

DTBS	Data to be Signed
SAD	Signer's Activation Data
SCD	Signature Creation Data
SCDev	Signature Creation Device
SCDId	Signature Creation Device Identifier
SSA	Server Signing Application

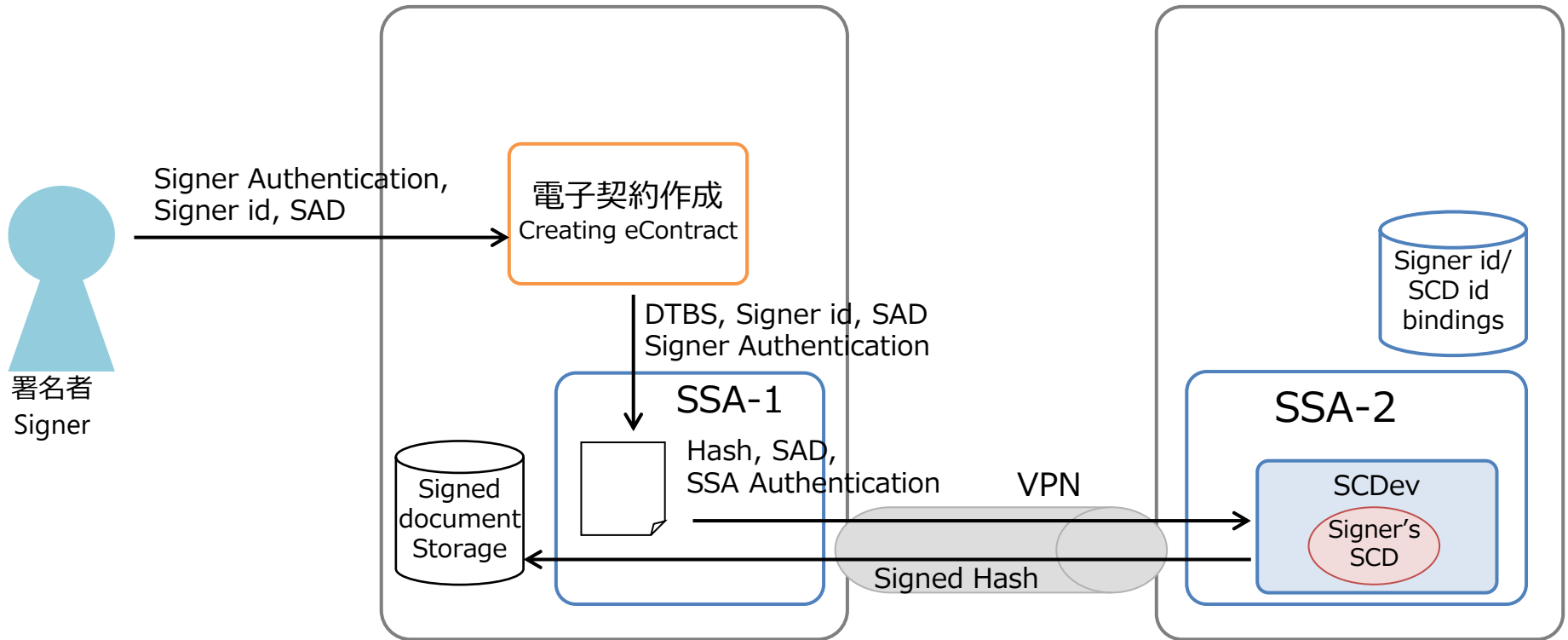
2. 国内サーバ署名事例構成②



■用語

DTBS	Data to be Signed
SAD	Signer's Activation Data
SCD	Signature Creation Data
SCDev	Signature Creation Device
SCDId	Signature Creation Device Identifier
SSA	Server Signing Application

2. 国内サーバ署名事例構成③



■用語

DTBS	Data to be Signed
SAD	Signer's Activation Data
SCD	Signature Creation Data
SCDev	Signature Creation Device
SCDid	Signature Creation Device Identifier
SSA	Server Signing Application