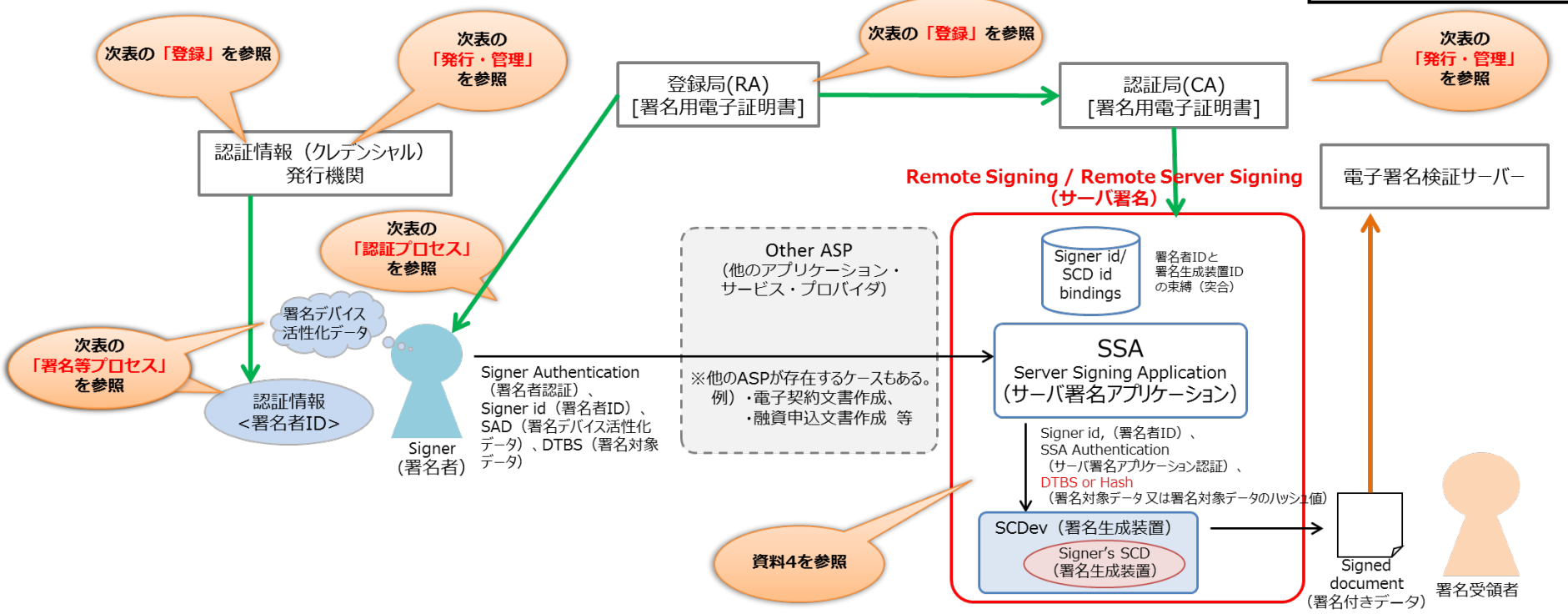
サーバ署名の構成要素とセキュリティ対策例

資料３



ガイドライン構成要素		保証レベル			
		1	2	3	4
申請等に係る厳格さ	※関連する基準として掲載	当該手続の申請等にあたり、特に確認を実施していない。	当該手続の申請等にあたり、本人確認又は申請書等の真正性確保のため、上記の方法ほどの厳格さはないが、何らかの確認を実施している	当該手続の申請等にあたり、本人確認又は申請書等の真正性確保のため、当該手続を所管する主体が保有するデータベースとの照合、もしくは公的証明書等による確認を実施している	当該手続の申請等にあたり、本人確認又は申請書等の真正性確保のため、当該手続を所管する主体が保有するデータベースに加え、主体以外が保有するデータベースとの照合を実施している、もしくは厳格な公的証明書等注による確認を実施している
登録	対面	◎電子メールアドレスが申請された場合、有効性（到達性）を確認する。	○左記と同等以上の対策基準とする。	○左記と同等以上の対策基準とする。	○左記と同等以上の対策基準とする。
			◎申請者は、公的な写真つきの身分証明書（運転免許証、パスポート等）を１種類、または、その他の身分証明書を２種類提示する。	◎左記と同等以上の対策基準とする。	◎左記と同等以上の対策基準とする。 ※２：公的な写真つきの身分証明書を必須とする
				◎申請者の氏名や住所等の公的な台帳との照合、または申請書に添付された公的証明書（住民票等）によりチェックする。	◎左記と同等以上の対策基準とする。 ※３：公的な台帳との照合を必須とする
					◎重複登録でないことを確認する。
	遠隔	◎電子メールアドレスが申請された場合、有効性（到達性）を確認する。	○左記と同等以上の対策基準とする。	○左記と同等以上の対策基準とする。	
			◎申請者の氏名と住所等、及び身元確認に有効な他機関の登録情報（クレジットカード番号等※２）が記載された申請書により申請する。	○左記と同等以上の対策基準とする。	
				◎申請者の氏名や住所等の公的な台帳との照合、または申請書に添付された公的証明書（住民票等）によりチェックする。	
				◎申請者の氏名と住所等が記載された申請書に本人の電子署名（郵送の場合は署名又は捺印）を付与して申請する。 ※電子署名は対象の保証レベルと同等の基準を満たすものの利用が望ましい。	
発行・管理	発行	◎認証情報及びトークンが、本人の電子メールアドレスに対して送付される。または、オンラインでの登録手続の過程で、本人が認証情報及びトークンをダウンロードする。	◎認証情報及びトークンが、以下のいずれかの方法により本人に配付される。 （１）窓口にて直接手渡される、 （２） ２つに分割され（例えば、ＩＤとパスワード等）、少なくともその１つが本人住所に普通郵便により送付される、 （３） 本人の電子メールアドレスに対して入手サイト先の情報とパスワードが通知され、本人が当該パスワードによる認証の上で、当該サイトからダウンロードする。	◎左記を任意基準とする。	◎認証情報及びトークンが窓口にて直接手渡される。（本人限定受取郵便基本型、及び同サービスと同等の手段による身元確認は対面として扱う）
	管理	◎検証者が使用する秘密情報（アカウント管理情報等）はアクセス制御によって保護され、パスワードのような秘密情報を平文のままで含まない。	◎左記と同等以上の対策基準とする。	◎左記と同等以上の対策基準とする。	◎左記と同等以上の対策基準とする。
	更新／再発行		◎認証情報及びトークンの更新、再発行に関する運用ポリシー（認証情報や登録情報等の更新の必要性や手続方法等）が策定され、周知されている。	◎レベル２と同等以上の対策基準に加え、特にオンラインによる手続の場合には、既存の認証情報及びトークンを用いた認証の上で、通信を暗号化して行なう。	◎レベル３と同等以上の対策基準とする。
	失効			◎認証情報及びトークンが有効ではなくなった、又は危殆化されたことを通知された時から、認証情報及びトークンを遅滞なく失効する。	◎レベル３と同等以上の対策基準とする。
	記録保管		◎認証情報及びトークンの発行、管理に関する記録を、当該認証情報の有効期限または失効時期の遅い方の時期から一定期間保管する。	◎レベル２と同等以上の対策基準に加えて、記録を定期的に分析、評価する。	◎左記に同じ
認証プロセス		◎オンライン上の推測、リプレイ攻撃	◎レベル1に追加し、 盗聴、セッション・ハイジャック （○中間者攻撃は強度に制約を設けても良い）	◎レベル2に追加し、 フィッシング／ファーミング （○中間者攻撃は強度に制約を設けても良い）	◎レベル3に追加し、 中間者攻撃（必須）
署名等プロセス	署名方式			◎電子政府推奨暗号リストに記載された公開鍵暗号による署名方式を用いること。	◎左記に同じ
	証明書用途の限定				◎電子署名用の証明書の用途を電子署名のみに限定すること。
	トークン（記憶された秘密など）			○攻撃者が有効な認証情報を推測できる確率（※２）は、トークンの有効期間を通じて２-10（1024分の１）未満とすること。	○左記を任意基準とする。
				◎攻撃者が有効な認証情報を推測できる確率は、２-14（16384分の１）未満とすること。	◎左記に同じ
	トークン（認証）			◎複数の認証要素を利用すること。	◎左記に同じ
					◎耐タンパ性（Common Criteriaによる EAL4+、又はJCMVPのセキュリティ評価に基づく耐タンパ性等）が確保されたハードウェアトークンを利用し、トークン・認証情報の複製に対し強い耐性を有すること。

インタビュー調査の結果
現状では、住民票、印鑑登録証明書、公的な台帳（名簿）の確認を実施（本人限定受取郵便を併用する場合もある）、レベル3及びレベル4のチェックを満たしていると考えられる。

インタビュー調査・議論の結果
レベル4の遠隔は、要調整。

「オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン、各府省情報化統括責任者（CIO）連絡会議決定、2010年」を基に作成
上記ガイドラインにおいて、◎は必須の対策基準、○は任意の対策基準、△は対策の強度に制約を設けても良い対策。