資料2

＜サーバ署名に求められる機能の一覧＞

主体	機能	規制の状況 日本	規制の状況 EU	規制の状況 米国	争点	求められる機能
本人	署名指示 （※海外では、電子署名に関する規制等）	現状、利用者が手元で署名	・Directive 1999/93/EC ・Regulation (EU) No 910/2014	グローバルな商取引と国内商取引における電子署名法（Electronic Signatures in Global and National Commerce Act（以下「ESIGN」という。））	署名指示者本人が確実に自らの意思において署名したという高度の蓋然性を確保できるかどうか？ （⇒電子署名法の法益）	本人だけが電子署名を行うことができる状態を確保した機能が必要
HSM サーバ署名	利用者登録機能 ※但し、初回に本人確認し、発行された利用者認証情報を登録する機能は別。	・ガイドラインP.32 ・署名法施行規則5条1項等	・Directive 1999/93/EC ・Regulation (EU) No 910/2014 ・EN 14169、TS 419-241	OMB M-04-04、SP800-63	国内ガイドラインのレベル3・4か？	現状の認定認証業務に準ずる
HSM サーバ署名	認証情報・トークンの発行・管理機能	・ガイドラインP.34 ・署名法施行規則6条3号等	同上	同上	国内ガイドラインのレベル3・4か？	現状の認定認証業務に準ずる
HSM サーバ署名	トークンの対策基準	ガイドラインP.40	同上	同上	国内ガイドラインのレベル3・4か？ （パスワード等に加えて、ICカード（マイナンバーカード等）も必須とするべきか）	本人だけが電子署名を行うことができる状態を確保した機能が必要
HSM	**鍵ペアの生成・管理機能** **【以下論点】**	**主要な法令改正検討対象**（または参考規程）	EUではまだ確定していない規程類が少なくない。	すでに確定し、運用も始まっている米国の規程類が、より参考になると思われる。		資料3参照
HSM サーバ署名	・署名生成鍵のインポートの可否	調査中				
HSM サーバ署名	・鍵の格納・管理	・署名法施行規則6条3号、3号の2，17号 ・署名法指針14条 ・署名法方針第4の2 ・金融機関におけるクラウド利用に関する有識者検討会報告書	・ETSI Workshop 資料 ・EN 14169、TS 419-241、 ・ELECTRONIC SIGNATURES Guide SEPTEMBER 2014	・ESIGN ・OMB M-04-04、SP800-63 ・AATL	・器機認証を取得したHSMを義務づけるか？ ・ソフトウェアレベルによる鍵ペアの作成・管理を（暫定的に）認めるか？ ・バックアップの方法・期間をどう考えるか？	署名法3条の3要件をクリアした機能であることが必要 ①符号の適正な管理を確保 ②本人だけが電子署名を行うことができる状態を確保 ③①、②を証拠として、後日検証することができる状態を確保
HSM サーバ署名	・利用する暗号の種類	署名法指針3条				
HSM サーバ署名	・鍵のライフサイクル管理	・署名法施行規則6条10号、12号、11条 ・金融機関におけるクラウド利用に関する有識者検討会報告書				
HSM サーバ署名	・バックアップの方法・期間等	調査中	Protection Profiles for TSP cryptographic modules（Part 1: Overview）、TS 419-241	調査中		資料4参照
HSM サーバ署名	※セキュリティ機能要件のレベル及び評価	ISO/IEC19790、 ISO/IEC15408	左記同じ	左記同じ （※FIPS140-2及び詳細規定）		
HSM サーバ署名	**署名機能** **【その他論点】** ・署名生成ログ管理 ・アクセス制御	ガイドラインP.47	Directive 1999/93/EC Regulation (EU) No 910/2014	ESIGN等	同上	同上
検証者	署名検証機能	署名法施行規則6条9号等	調査中	調査中	特段ないのでは？	現状の認定認証業務に準ずる。

資料5参照

※ISO/IEC 19790は、FIPS 140-2のDTR、IGを取り込みISO/IEC 24759:2008（現在、ISO/IEC 24759:2013をJIS化）
※EN 14169：ETSI Standard 14169：Protection profiles for secure signature creation device、
※TS 419-241：ETSI Technical Specification 419-241：Security requirements for trustworthy systems supporting server signing (signature generation services)
※EN 419-221：ETSI Standard 419-221 Security requirements for trustworthy systems managing certificates for electronic signatures
※OMB M-04-04：連邦政府機関向けの電子認証に関わるガイダンス
※SP800-63：NIST Special Publication 800-63：電子認証に関するガイドライン