資料4

サーバ署名における鍵管理・本人性確認の考え方について（現行電子署名制度との比較）

秘密鍵の管理		発行者署名符号の管理 （※発行者署名符号：電子証明書の発行者である機構の秘密鍵）	
現状の電子署名制度	サーバ署名における考え方	現状の電子署名制度	サーバ署名における考え方
利用者の鍵ペアの発行を認証事業者に郵送で依頼する場合			
＜施行規則6条3号＞ ○認証事業者が秘密鍵を作成する場合、当該秘密鍵を利用者に安全かつ確実に渡すことができる方法により交付又は送付する。 ○当該秘密鍵及びその複製を直ちに消去する。	**＜以下の要件①～③を必要とする（★）＞** **①（HSMの活用）**認証事業者が鍵ペアを作成する場合、高度な暗号演算処理等を安全かつ安定的に行うことができると米国FIPS140-2（※1）の認定を得たHSM（※2）で鍵ペアを作成・保管する（※3）。 （※1）連邦情報処理規格。米国連邦政府機関が軍事以外の用途で購買・利用する情報・通信機器が満たすべき技術標準を定めた規格 （※2）Hardware Security Module。鍵ペアを物理的に守る金庫のような役目をする高機能なハードウェアであり、秘密鍵を一切外に出さずに暗号、電子署名等の処理を行うことができる。 （※3）当該暗号演算処理等は、技術的にはソフトウェアレベルでも行うことができるところ、米国の事業者での事例もあり、また、現在EUでも規定化に向けた検討が行われている（今夏頃メドに結論が出る予定）。 （→暫定的（2～3年程度）にソフトウェアレベルでの暗号演算処理等を認めるかは第3回の研究会で議論する予定）。 **②（本人性確認を厳重に）**鍵ペアは、認証事業者のサーバ等にとどまるが、その取扱いについて厳重に業務規程を課した上で、物理的にも当該鍵ペアの利用（活性化）には、利用者本人しか知り得ない要素（※4）を必要とする（※5）。 （※4）当該要素は、いわゆる二要素認証（例えば、①マイナンバーカード等高度の本人確認機能を有するカード、②パスワードやPIN等）とする。） （※5）本人の意思を確認するポップアップを表示し、「はい」ボタンの押下も必要とする。 **③（データの証拠力の担保）**一定期間、鍵ペアや利用者認証等のデータのバックアップ・ログをとることとする。	＜施行規則6条17号＞ ○複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止するために必要な措置が講じられていること。 ＜特定認証業務の認定に係る指針14条＞ ○認証設備室内で複数の者によって専用の電子計算機を用いて行われること。 ○バックアップ用の発行者署名符号の複製は、次のいずれかの方法により行われること。 ・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。 ・認証設備室内で発行者署名符号に関する情報を分割し、複数の者が異なる安全な場所に分散して保管する方法により行われること。 ○認証業務用設備の設定の変更は、認証設備室内で複数の者により行われること。 ○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等の方法により完全に廃棄し、かつ、複製された発行者署名符号についても同時に廃棄すること。	**※特に左記と相違点はない。**
利用者が自ら鍵ペアを発行する場合			
＜施行規則6条3号の2＞ ○ブラウザ等を通じて利用者が秘密鍵を作成する場合、認証事業者は利用者識別符号（1回限りの識別に用いる符号。いわゆるワンタイムURL等）をあらかじめ安全かつ確実に利用者に交付又は送付する。 ○利用者以外の者が当該符号を知り得ないようにする。	○施行規則6条3号は鍵ペアの発行を郵送等により認証事業者に依頼する場合の考え方であり、施行規則6条3号の2は利用者がブラウザ等（USBトークンを利用し、パソコン上で作業するような場合も含む。以下同じ。）を通じて自ら作成するものである。	**※上記と同様**	**※特に左記と相違点はない。**
＜指定調査機関の調査に関する方針第4の2(1)＞ ○認証設備室又は同等の安全性が確保できる環境において、複数人で秘密鍵を作成する。 ○秘密鍵の転送や出力等の取扱いは、作成時と同等の安全性を確保する。 ○秘密鍵を利用者に交付又は送付したときは、受領書等を受領する。			
＜指定調査機関の調査に関する方針第4の2(2)＞ ○当該符号は、安全な乱数生成アルゴリズムを用いて生成し、認証設備室等において複数人で行う。 ○当該符号の受領確認を行った上で、利用者に電子証明書を発行する。 ○当該符号は、認証設備室等に暗号化等の措置を講じて保管する。 ○利用者が当該符号を送信する際には、通信に暗号化等の措置を講じる。 ○当該符号の利用があくまで一度きりであるように措置を講じる。	○利用者が当該鍵ペアの作成をブラウザ等を通じて行うことのリスクへの対応策として、施行規則6条3号の2及び方針第4の2(2)が規定されているわけであり、上記①～③及び左記の要件を満たせば（※6）、サーバ署名においても当該作成をブラウザ等を通じて行うことは認められると考えられる。 （※6）具体的な実施方法に合わせた適切な対策（要件の詳細化）が必要（**→資料5の2-3参照**）。 － サーバ署名事業者の環境で鍵ペアを生成する場合 － サーバ署名利用者の環境で鍵ペアを生成し、サーバ署名事業者に送付する場合		