（参考）メールでの追加コメント

（小田嶋委員）

＜モダナイズの方向性❹に関する議論＞

A)認証局のリポジトリにおける利用

電子署名法に於いて、リポジトリサーバーにより、認証事業者が万人に対して情報公開を義務付ける情報を 4 項目の調査表項番で定めている。関連する調査表項番の 4 項目を以下に具体的に列挙する。

【1】調査表項番 3513：

(3)当該発行者署名符号に対応した発行者署名検証符号に係る電子証明書の値を SHA-256、SHA-384 又は SHA-512 のうちいずれか 1 以上で変換した値（フィンガープリント）を記録し、改ざん防止措置を講じて公開している。

【2】調査表項番 3901：

(1) 以下の(2)～(13)の事項に関して、認証業務規程に明確かつ適切に規定し、電磁的方法により記録し公開している。

【3】調査表項番 3907：

(7) 電子証明書の失効情報の確認方法及び期間に関する事項① 公開される失効に係る情報の内容及び公開の方法、電子証明書の失効情報の更新の周期② 失効に係る電子証明書の利用者への通知方法③ 有効期間の経過後に署名検証者からの電子証明書の失効に関する情報について照会を受けた場合の対応方法等

【4】調査表項番 3712：

(2) 以下の①～③の事項を含む署名検証者に対する説明事項をわかりやすく記述し、電子証明書のリンク先等の場所に掲載している。① 発行者署名検証符号及びフィンガープリントを確実に入手し、電子証明書に行われた発行者による電子署名を検証することにより、電子証明書の発行者を確認すべきであること。② 電子証明書を信頼すべきか否かの判断する際は、電子証明書の利用目的もしくは使用範囲又はその制限（利用者に通知した利用条件を含む。）を確認すべきであること。③ 適切な手段を用い、電子証明書について失効されていないことを確認すべきであること。

実際には、【1】～【3】は認証事業者が公開する情報を定め、【4】（項番 3712）は利用者がリポジトリサーバーで公開された情報を使用して確認する①～③の項目として定めているが、【1】は厳密には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の公開のことしか触れられていないが、実際には【4】の利用者の義務を満たすためには、発行者署名検証符号に係る電子証明書を公開して利用者が入手可能にすることも必須であり、発行者署名検証符号に係る電子証明書の公開も事実上要件となっている。結論として、認定認証事業者には、利用者が確認可能なようにリポジトリサーバーで公開すべき義務を持つ情報を調査表項番 3513、3901、3907 の 3 項目に定めており、認定認証事業者に課せられる要件は以下の【1】～【3】の 3 項目に限られている。その要件の本質は【公開していること】であって、リポジトリサーバーはメンテナンス時に計画停止を行うことが通常の運用

であり、鍵更新や相互認証証明書更新の実施の日には、1 日程度の停止が行われている実態がある。指定調査機関は可用性や災害時の復旧対策について、その実施内容を認定調査の一つとして確認はしているが、稼働率などの具体的な数値レベルの要件は存在せず、一般論的に適切な実施であれば、問題とされることはない。（例として、メンテナンス等は BCA へ事前連絡することとなっている）

【1】発行者署名検証符号と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の公開
【2】認証業務規程（CPS）の公開
【3】失効情報（ARL/CRL）の公開

このような現状、公開されていることが電子署名法の要件のリポジトリサーバーの要件に、オンプレの場合には課せられなかった要件がクラウド利用の場合にのみ可用性に係る要件として、稼働率や停止時間の数値要件を定める形となるのは過剰であり、適切なものとは言い難いと考える。

【参考】AWS の例になるが、クラウド利用時に設定する項目として、動作するリージョン設定を行うが、当該リージョンでのクラウドの起動タイプと呼ばれるパラメータを適切なリソースを利用するように自動化される FARGATE と呼ばれる方式を指定するように推奨している。当該リージョン内には、最初から最低３つ以上のアベイラビリティゾーンが割り当てられており、その割り当て数やクラスタ、タスク、サービス等と呼ばれる実行単位のインスタンスのアベイラビリティゾーンへの割当方法をあたかも人間が管理のために設定したものとして、管理画面などで確認しても意味を持たないし、その必要性もないと考える。

＜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の公開方法＞

電子署名法に於いて前述のとおり、リポジトリサーバーにより、認定認証事業者が万人に対して情報公開を義務付ける情報を調査表項番にて定めているが、その一つが調査表項番 3513 において「発行者署名検証符号に係る電子証明書（CA 証明書）を SHA-256、SHA-384 又は SHA-512 のうちいずれか 1 以上で変換した値（フィンガープリント）を記録し、改ざん防止措置を講じて公開している。」と定めている通りに公開している。このフィンガープリントの公開に当たっては、改ざん防止措置を講じることが要件とされている。この調査表項番 3513 の記載に基づいて、各社とも改ざん防止措置ツール／ソフトウェアや改ざん検知ソリューション／サービスを導入して、フィンガープリントを公開する Web サイトのページの改ざん検知を実施している。

一方、リポジトリでの公開義務のある発行者署名検証符号に係る電子証明書（CA 証明書）、及び失効情報（CRL）の公開に当たっては、発行者署名符号（CA 秘密鍵）による自己署名が付与されるため、電子署名による改ざん検知が可能となっている。

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の公開に際しては、調査表項番 3513 の措置として明記されたことにより、改ざん検知ツール／サービスの導入による改ざん防止措置を実施することが事業者の義務の如くなっている実態がある。

然るに、発行者署名検証符号に係る電子証明書（CA 証明書）、及び失効情報（CRL）のように電子署名による改ざん防止措置を施すこと、例えばフィンガープリントの文字列を記載した PDF ファ

イルに発行者署名符号（CA 秘密鍵）による署名を付与して公開することでも、改ざん防止措置を施すことが可能となるのではないかと考えられる。今一度、発行者署名符号（CA 秘密鍵）による自己署名による改ざん防止措置を容認できるよう、調査表項番 3513 に追記する検討を進めて頂きたい。

B)利用者の申込み／利用者の本人確認における利用、および
D)認証局の帳簿書類等の保管のクラウド化、に関する意見

46 スライド目の ISO27000 シリーズ、とくに ISO27017（クラウドセキュリティ）は ISMS のセキュリティ基準そのものであり、表現がおかしい。ここで議論すべきは、クラウドセキュリティの議論のところに、ISMAP のガバナンス基準を持ち出すことの是非であり、ガバナンス基準は切り離して❶として独立して議論すべきと考える。

C)認証局の保守・運用における利用

44 スライド目の最下行「インターネットとは独立した専用の監視 NW を利用した遠隔操作」は、「データセンター」「死活監視サービス」「クラウドサービス」の各サービサーが共存するので、本文の 2 ポツ目の文中に出てくる CSP は「CSP 等」とするのが適切と考える。

以上