様式

意 見 書

平成 20 年 3 月 24 日

総務省情報通信政策局
　情報流通振興課　御中
法務省民事局
　商事課　御中
経済産業省商務情報政策局
　情報セキュリティ政策室　御中

郵便番号　：　163-0430
（ふりがな）　とうきょうとしんじゅくく　にししんじゅく
住　　所：東京都新宿区西新宿 2-1-1
　　新宿三井ビル 30 階
（ふりがな）　でんしにんしょうきょくかいぎ
名　　称：電子認証局会議
（ふりがな）　まきのじろう
代表者氏名：牧野二郎
電話番号　：　03-5339-2776
電子メールアドレス　：makino@makino-law.jp

電子署名及び認証業務に関する法律の施行状況に係る検討会報告書（案）に関し、別紙のとおり意見を提出します。

（別紙）

「電子署名及び認証業務に関する法律の施行状況に係る検討会」報告書（案）
『意見書』

＜意見総論＞

電子署名法の見直しということについて、次の3つの観点を調和させて、円滑に移行できる対応計画を立案いただきたい。

1. 暗号技術の危殆化に対する論理的・技術的視点での対応必要性
2. 電子署名・認証の用途・目的に応じた具体的脅威を認識しての対応必要性
3. 認定認証局が実施する認証範囲の再標準化の必要性

暗号技術の危殆化に伴う、電子署名法上の規則及び告示の改正は、電子認証局の変更認定や新規構築等に連動し普及しつつあるアプリケーションの改良を強制することになる。
前提として現行の認証局の認証基盤によって動作している多くのアプリケーション運営者や利用者に対し「暗号技術危殆化に対する具体的脅威の共通認識」を明示して理解を得ることが重要と考える。

また、暗号アルゴリズムの移行がスケジュリングされれば同法に基づく認証局は認証局システムの改変を行わねばならない。

- 早急に認定認証局へのヒアリングや啓発活動が要されると考える。
- 電子署名法の変更認定にかかる対応方法やスケジュールは早期に公示いただきたい。

政府のリーダーシップによって、認証局の EE 証明書を使用する全てのアプリケーションは、認証基盤の移行に先行して一定期間内に移行していくような体制を敷いていただくことが必要と考える。アプリケーション運営者へは、暗号技術に対する下位互換を保証して移行することを認識いただく必要性もある。既に稼働しているアプリケーションや電子署名を付された電磁的記録に対する円滑な移行対応を可能とするよう留意いただきたい。

尚、移行については、国のみならず LGPKI や公的個人認証など地方自治体等の情報システム側の対応も足並みをそろえていただくことが重要であると考える。

また、認定認証業務の電子証明書に記載する所属組織名などの属性情報の標準化や認定範囲についても合わせて検討する必要があると考える。

◆意見－1

＜該当箇所＞

第2章 検討結果

1．電子署名に用いる暗号技術の安全性向上に係る方策について（技術的論点）

（3）背景

・ ハッシュ関数の安全性に係る状況

・ SHA-1 における衝突計算攻撃に要する時間の推定

＜意見内容＞

SHA-1の安全性低下が「具体的にどのような場面でどのように何が危険なのか」リスク分析の結果が明確ではないと考えます。実際に有意な攻撃に対するリスクや攻撃に要するコストなども評価し、それが現実的な脅威となりうるのか？など、一般国民に納得いくような、本件移行計画の背景にある具体的リスクの掲示をお願いしたい。

＜理由＞

暗号アルゴリズムの移行は、長期的には避けて通れない道であることは指針で示される通りだが、影響が広範囲に及ぶこともあり、対策の適時、適切な範囲を判断する上で、どのような脅威に対し、どの範囲で対策を講ずるべきなのかを明確にする必要が有ると考える。

本報告書では、具体的にどのような場面でどのように何が危険なのか？リスク分析の結果が明確ではないと考える。

・複数の異なる文書に同一の電子署名が付される脅威（衝突計算攻撃）

・電子署名が付された電子文書と同一の電子署名が別の電子文書に付される脅威（第二原像計算攻撃）

が示されているが、

① 複数の異なる文書に同一の電子署名が付される脅威（衝突計算攻撃）

衝突計算攻撃が実際に優位な攻撃となる事は、どのような場合が考えられるのか？単にSHA-1の衝突性を発見するだけでなく、その2つの確率より遙かに低くなることが想像できる。

② 電子署名が付された電子文書と同一の電子署名が別の電子文書に付される脅威（第二原像計算攻撃）

署名者が故意に2つの異なる文書に同一の電子署名を付す事が考えられ、否認防止機能が働かなくなる恐れが出てくる。これは実際の脅威になり得ると考える。

実際に有意な攻撃に対するリスクを想定する場合、②の第二原像計算攻撃を想定するのが合理的ではないか？その場合の計算量はこの報告書では示されていないが、衝突発見の計算

量の“２の６９乗”より遙かに大きいのではないか？

◆意見－2
＜該当個所＞
第2章　検討結果
1．電子署名に用いる暗号技術の安全性向上に係る方策について（技術的論点）
(4)検討結果
○SHA-1、RSA1024bitに基づく電子署名を将来、無効とする旨を、どのように規定すべきか
．．．前略
P16
「衝突計算攻撃に要する時間の推定に関しては、2006 年6月時点において、国内最高速のスーパーコンピュータを用いれば 462 年以下で衝突発見されるおそれがあることが示されている。一方、第二原像計算攻撃に関しては、現時点において報告されてはいない・・」

＜意見内容＞
数学的な脅威は感じられても、電子認証・電子署名の「①なりすまし防止②盗み見・盗聴防止③改竄防止④事後否認防止」という機能に対し、どの機能が具体的にどの程度まで危険性が出るのかアプリケーション運営者や利用者には理解不能である。
早急に関係者へのヒアリングや啓発活動が要されると考える。
＜アプリケーション運営者の例＞
：電子入札・申請システム運営の国や地方公共団、BtoB の EC システム運営者
＜利用者の例＞
：電子入札対応者、電子申請利用者、電子商取引利用者

◆意見－3
＜該当箇所＞
第2章　検討結果
1．電子署名に用いる暗号技術の安全性向上に係る方策について（技術的論点）
(4)検討結果
○SHA-1、RSA1024bitに基づく電子署名を将来、無効とする旨を、どのように規定すべきか
．．．前略
P－17
・電子署名付き文書に対する対策（例：再署名、タイムスタンプ等）

＜意見内容＞

署名に用いられる暗号アルゴリズムの脆弱化に対応し、暗号アルゴリズムの切替え後署名検証が継続できる署名形式の採用を、追記すべき

(修分例)

・電子署名付き文書に対する対策(例:再署名、タイムスタンプ、長期署名方式、等)

＜理由＞

旧アルゴリズム使用禁止日時以降も署名検証には旧アルゴリズムを使用できなければならないが、旧アルゴリズム単独での利用は脆弱となる。これを防止する有効な手段として、RFC3126 に準拠した長期署名フォーマットがあり、より強固な暗号アルゴリズムを用いたタイムスタンプを用いて、署名文書と検証情報(署名者や認証局などの関連する証明書や失効情報を指す)を保護することにより、証明書の有効期限や署名の暗号アルゴリズムの安全性低下を越えて、電子署名の有効性が検証できる。さらに、この規格はECOMからJIS化提案がなされ、この3／21付け官報(号外第57号)にてJIS化が公表された(JIS X5092、及びX5093)。対応製品も市場に複数種類あり、普及に問題無い状況にある。

◆意見－4

＜該当箇所＞

第2章 検討結果

1.電子署名に用いる暗号技術の安全性向上に係る方策について(技術的論点)

(4)検討結果

○SHA-1、RSA1024bitに基づく電子署名を将来、無効とする旨を、どのように規定すべきか

P16、17

2014年度 末前後を目途	SHA-1、RSA1024bitによる利用者電子証明書の有効期間後に、特定認証業務に係る電子署名の基準から、SHA-1、RSA1024bitを削除。 (SHA-1、RSA1024bitによる利用者電子証明書の有効期間について、各認定認証事業者は、SHA-2、RSA2048bitによる利用者電子証明書への切替を考慮し、あらかじめ調整を図ること等が求められる)

＜意見内容＞

以下を削除

(SHA-1、RSA1024bit による利用者電子証明書の有効期間について、各認定認証事業者は、SHA-2、RSA2048bit による利用者電子証明書への切替を考慮し、あらかじめ調整を図ること等が求められる)

＜理由＞

新アルゴリズムの証明書発行以後は、旧アルゴリズムの証明書の有効期間がまだ残っていることを認めない意図が読み取れる。この報告書の段階ではそこまで踏む込むべきではなく、移行の具体的な内容については、認証事業者やアプリ運営者等の関係者から広く意見を聞いた後に決定しても良いのではないか？

◆意見－5

＜該当箇所＞

第2章　検討結果

1．電子署名に用いる暗号技術の安全性向上に係る方策について（技術的論点）

(4)検討結果

○SHA-1、RSA1024bitに基づく電子署名を将来、無効とする旨を、どのように規定すべきか

P16

スケジュール案

＜意見内容＞

新アルゴリズムへのスムーズな移行のために以下をご留意いただきたい

① 認証局の鍵更新での留意事項

- アルゴリズムの脆弱化に伴う認証局鍵更新
  RSA2048bit を使用している認証局証明書は、ハッシュに SHA1を用いていたとしても、アルゴリズムの脆弱化だけが理由で鍵更新を行う必要は無い。
- 鍵更新後の認証局証明書の取扱い
  移行スケジュール確定以前から旧アルゴリズム使用禁止日時以降まで有効期間があるCA証明書を持つ認証局が、移行対象となる暗号アルゴリズムで運用している場合は、旧アルゴリズム使用禁止日時以降、私有鍵を新たな電子署名に利用してはならないが、暗号アルゴリズム脆弱化理由での失効処理は行うべきでない。
  尚、旧アルゴリズム使用禁止日時を越えて署名検証が必要となる場合は、その時点で有効なすべての電子署名対象文書に前述の長期署名を施し、署名検証が可能な状態を維持する必要がある事に留意されたい。

② 加入者証明書の取り扱い（旧アルゴリズム使用禁止の運用開始時期）について

- 暗号アルゴリズム脆弱化理由での失効処理は行うべきでない。十分余裕のある移行スケジュールをご検討いただきたい。

＜理由＞

① 認証局の鍵更新での留意事項

- アルゴリズムの脆弱化に伴う認証局鍵更新
  SHA1の衝突性の問題が指摘されているが、認証局でハッシュを作成する場合であって、暗号アルゴリズムに RSA2048 を用いる場合は、SHA1 と RSA2048 を組み合わせて利用する事は問題無いと考える。（この根拠は意見－1の理由）
- 鍵更新後の旧認証局証明書の取扱い。
  長期署名フォーマットを採用していない場合に限るが、認証局証明書の取消処理を行うと、当時に発行した証明書を用いた過去の署名データが検証不能となり、混乱をまねく。新アルゴリズム移行後は、むしろ旧認証局の公開鍵証明書にタイムスタンプを付与するなどして、真正性を保って保管することなどが必要となる。

② 加入者証明書の取り扱いについて

- 発行済み証明書を想定外に大量に取消す場合、以後の署名検証が不可となり混乱を生じる。想定外の証明取り消しは出来る限り避けるべきである。

◆意見－6

＜該当箇所＞

第2章 検討結果

4. その他の諸課題

(2) 認定認証業務の電子証明書に記載する属性情報

＜意見内容＞

電子証明書の属性項目や審査レベルに関する標準化、もしくは、それを促す指針の策定が必要である。

＜理由＞

各府省における電子申請等システムの条件として、法人として利用する場合、利用する電子証明書には法人名および法人代表者名を必須とするものが多い。現在は各認証事業者が個々に設定しており、その都度対応するクライアントソフト開発ベンダの負担も大きいと考えられるため、電子証明書の属性項目や審査レベルに関する標準化が必要であると思われる。

◆意見－7

＜該当箇所＞

第2章 検討結果

4. その他の諸課題

（2） 認定認証業務の電子証明書に記載する属性情報

＜意見内容＞

電子証明書に記載する氏名・住所・生年月日以外の属性の証明について認定の対象に含める場合には、一律の適用ではなく、認定認証業務を行う認証事業者が、属性の証明に係る業務について認定認証を受けるか受けないかの選択を行うことが可能となるようお願いしたい。

＜理由＞

現時点で既に、認定認証業務を行う一部の電子認証局が発行する電子証明書には、電子証明書の名義人が所属する組織等の名称と所在地が記載されている。これは、主に国土交通省等で実施されている電子入札コアシステムの要件に対応するためである。記載内容の確認に用いる資料としては、法務局に登記可能な組織あれば、登録事項証明書を以って確認しているが、所謂、個人事業者など法務局に登記されていない組織の場合は登録事項証明書がないため、複数の資料の確認が必要となる場合があり、認証事業者及び電子証明書利用者双方にとっての負担が少なくない。仮に属性情報が認定対象となる場合は、一部の利用者について、電子証明書を発行できないといった事象が懸念され、円滑な電子署名の普及の足かせとなる可能性がある。

このため、属性情報の確認業務については認定を受けずに現行と同様の確認手段を以って確認された電子証明書と、今般ご検討の属性情報の確認業務についても認定を受けているという認証事業者が存在し、電子証明書を利用する側がいずれの電子証明書を利用するのかの選択肢があるようご検討いただきたい。

◆意見－8

＜該当箇所＞

第2章　検討結果

4．その他の諸課題

(3)電子署名の長期検証性の確保

P-23

■　考え方

電子署名法は、電子署名の法的取扱いを確立することを目的としており、これに関して必要な事項を定めるもの。電子署名をどのように利用するかについては、市場の活動を制限しないという観点からも特に規定しておらず、電子文書の長期保存に利用する場合の措置に関する規定を置くことも考えにくい。しかしながら、電子署名をとりまく環境の整備という視点から、主務省は、電子署名の長期検証を可能とする各種技術の開発・標準化等を支援していくことが適当。

＜意見内容＞

前略・・・・・・。しかしながら、署名検証の継続に関しては留意する事が必要であり、電子署名をとりまく環境の整備という視点から、主務省は、電子署名の長期検証を可能とするガイドラインの整備、各種技術の開発・標準化等を支援していくことが適当。

＜理由＞

電子署名は、それが（署名法の要件を満たしていることを）正しく検証できて初めて効力を発揮すると考える。電子署名データ自身の検証可能期間は証明書の有効期間内に限定されことから、少なくとも、署名対象文書の真正性の維持が必要な期間は署名検証を維持する手段を提供できることに留意が必要となる。例えば、「政府機関の情報セキュリティ対策のための統一基準(第 3 版)解説書 4.1.6 暗号と電子署名」でも示されているように、署名検証の継続性の確保を署名の基本要件として、ガイドライン等で明記し、加入者、利用者間で広くコンセンサス形成を図ることが重要であると考える。