様式

【意 見 書 要 旨】

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したので、その要旨のみここに表示いたします。

電子認証局会議　意見書　【要旨】

意見総論部分要旨

電子認証局会議としては、認証局の運営、認証業務の活用を促進する立場から、次の通り考える。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

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、これを利用する多くの利用者に対し「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。そのためにも、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くこと、また、アプリケーション運営者は、暗号技術に対する下位互換を保証して移行する必要性もある。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、政府の指導力を発揮されたい。

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。

意見部分要旨（基本的に本文の通りである）

1　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、攻撃のコストの評価、現実的な脅威の内容を明確にすべきである。

2　数学的な脅威はともかくとして、電子認証・署名の機能の、どの部分に、どの程度の危険が生じるのか、アプリケーション変更の必要性があるか、の検討が必要である。

3　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(例えば再署名、タイムスタンプ、長期署名方式等)を、追記すべきである。

4　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記載部分は削除すべきである。

5　新アルゴリズムへの移行に際しては①認証局の鍵更新、②加入者証明書の取り扱いについて留意すべきである。

6　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。

7　属性証明を認定の対象とする場合に、一律とせず、選択的方式を採用すべきである。

8　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整備、各種技術の開発・標準化等を支援していくことが必要であり、その旨明記すべきである。