

内閣官房情報セキュリティセンター御中

(政府機関総合対策促進担当)

齊藤参事官補佐、本多 殿

「政府機関の情報システムにおいて使用されている暗号アルゴリズム  
SHA-1 及び RSA1024 に係る移行指針」(案) に対する意見書

2008年3月19日

名称: 電子認証局会議

代表者氏名: 牧野二郎

主たる事務所の所在地: 〒163-0430 東京都新宿区西新宿 2-1-1 新宿三井ビル 30 階

牧野総合法律事務所、電子認証局会議事務局

連絡先

連絡担当者氏名: 弁護士牧野二郎

電話番号: 03-5339-2776

メールアドレス: makino@makino-law.jp

すでに実施されました表記移行指針(案)に対するパブリックコメントに対して意見として提出すべきものでありますが、当方の手続きミスにより、提出期限にかないませんでしたので、あらためて、上記指針(案)に対する意見書の提出として、本意見書を提出させていただきます。

本意見は、電子認証局会議として議論の末、決定したものであり、当会議の意見としてご理解、御検討賜りたく、お願い申し上げます。

当会としては引き続き、移行に関する検討を重ねると共に、前記移行指針(案)に対しても建設的な議論を進めた参る所存であります。

なお、形式としましては、前記パブリックコメントへの意見陳述の形式を取らせていただきます。

重ねてお詫びし、お許しいただきますようお願い申し上げます。

<該当箇所1>

1 はじめに、

前略…、これらの暗号アルゴリズムについて、情報システムのライフサイクル等をふまえて、適時により安全なものに移行する必要がある。

<意見内容1>

「暗号アルゴリズムの安全性低下」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。例えば、SHA-1の衝突性が当初想定されたよりも高いと評価されていても、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揭示をお願いしたい。

<理由1>

本指針は事実上、政府機関の情報システムに留まらず広く我国PKI全体での「移行計画」に影響するものであると考えます。

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お示しの通りですが、本指針の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ます。

<該当箇所2>

3 内容、(1)情報システムの設計要件、及び

3 内容、(2)計画の策定 イ

<意見内容2>

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

<理由2>

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2月に承認されており普及に問題無い状況にある。

<該当箇所3>

3 内容、(2)計画等の策定 イ、ウ、及び

3 内容、(3)スケジュール

<意見内容3>

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3>

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。

- ・ 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。

<該当箇所4>

3 内容 (1) 情報システムの設計要件 ウ ア及びイ以外の情報システム

<意見内容4>

本指針の範囲を明確にしていきたい。

- ① 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ます。
- ② SSLのWebサーバ証明書は電子署名法の対象外ではありますが、SHA1 及び RSA1024 が使用されている場合、本移行指針の対象となるのかどうかは明確ではありません。この点を明らかにしていきたい。
- ③ また、民間の認定認証局や、電子申請に関連する署名アプリケーション等は対象となるのでしょうか？

<理由4>

- ① GPKI、LGPKI、公的個人認証基盤などの公的認証基盤において、暗号技術の信頼性は異なるべきでなく整合性を持つ必要が有ると考えます。
- ② Webサーバ証明書まで対象とした場合、ブラウザとしてケータイまで考えた場合、署名検証アルゴリズムの置換えは利用者の新機種への買い替えを待つしかありませんので、移行期間が長くなります。注意が必要かと思われます。署名目的に限るのか、サーバ認証、クライアント認証にも適用されるのかを明らかにしていただくようお願いします。
- ③ また、e-Gov の電子申請に用いられる電子証明書を発行する民間の認定認証局や関連するPKI アプリケーションなども、この指針の範囲に含まれるのか明らかにしていただくようお願いします。