

「政府機関の使用している暗号アルゴリズムSHA-1及びRSA1024に係る
移行指針」(案)に対する提出意見の概要及び御意見に対する考え方
(案)

情報セキュリティ政策会議
平成 年 月 日

意見提出者一覧（五十音順）

財団法人 日本データ通信協会 タイムビジネス協議会

特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG

日本クロストラスト株式会社

「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)
 に対する提出意見の概要及び御意見に対する考え方(案)

該当箇所	御意見の概要	御意見に対する考え方
3 内容 (1) 情報システムの設計要件 ア 政府認証基盤 (GPKI)及び 商業登記認証局 (イ)	商業登記認証局のOCSPの署名に関して、現状のOCSPの標準であるRFC 2560では、SHA-1以外のハッシュアルゴリズムを利用できるようになっていないが、複数のアルゴリズムを選択可能とする仕組みを、どのように実装する予定か、また、GPKIの証明書検証サーバもOCSPベースの独自プロトコルとなっているが、今後ハッシュアルゴリズムが交換可能となるのか、この際、ハッシュアルゴリズムの交換が可能であるRFC 5055 SCVPへ移行も検討するべきではないか、「公開鍵暗号方式」に関して、認証局の自己署名証明書は、海外の事例でも、RSA2048以上の鍵長を持った自己署名証明書が多数見受けられるところ、自己署名証明書は、証明書の検証要件として、RSA2048以上のRSA3072、RSA4096の検証も可能とすることを検討すべきではないか。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	今回の指針に従って決定すべき具体的な技術要件については、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。 なお、RSA鍵長が2048以上のものについては、指針では、「以下の暗号アルゴリズムを含める」とありますので、指針はそれらアルゴリズムを用いた署名検証を妨げるものではありません。
3 内容 (1) 情報システムの設計要件 ア 政府認証基盤 (GPKI)及び 商業登記認証局 ア及び イ 政府認証基盤に依存する 情報システム	移行指針の適用範囲が不明瞭。証明書を発行する認証局として、LGPKI、JPKIなどの認証局は含まれるのか、総務省運用支援認証局等は含まれるのか。さらに「イ 政府認証基盤に依存するシステム」として、電子政府のWebサーバや、JPKIなどで利用されているコード署名などの扱いを明確にするようお願いする。また、政府認証基盤 (GPKI)には、民間の認証局も接続されている。こうした民間側の扱いについても明確にするようお願いしたい。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	指針案の本文「2 対象機関」において、対象を記載してあるように、政府機関を対象としていることから、LGPKI、民間認証局等は本指針の対象となりません。また、「電子政府のWebサーバ」の証明書はGPKIと相互認証していないので、「ウ ア及びイ以外の情報システム」に該当します。
3 内容 (1) 情報システムの設計要件 イ 政府認証基盤に依存する 情報システム (フ)	文書ファイルへの電子署名に関して、署名者自身による攻撃は、Second-Pre-Image攻撃(第二原像計算攻撃)で想定される計算量よりも少ない計算量で成立する可能性がある。このため、RSA1024とSHA-1に関して、文書ファイルへの電子署名、電子証明書、それぞれの根拠を明確にして、その移行時期を検討するべき。また既存の署名文書に対する方針も検討するべき。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	今回の指針に従って決定すべき具体的なスケジュールについては、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。
3 内容 (1) 情報システムの設計要件 イ 政府認証基盤に依存する 情報システム ア及び ウ ア及びイ以外の情報システム	情報システムの設計要件において、将来の暗号アルゴリズムの脆弱性に起因する電子署名付き文書ファイル及び電子証明書の信頼性の消失の脅威に備えるために、ETSI TS 101 733 CMS Advanced Electronic Signatures (CAAdES)方式あるいはETSI TS 101 903 XML Advanced Electronic Signatures (XAAdES)方式等の電子署名を付すことを推奨されるよう追記すべきと考える。 【財団法人 日本データ通信協会 タイムビジネス協議会】	今回の指針に従って決定すべき具体的な技術要件については、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。
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	移行指針の「ウ ア及びイ以外の情報システム」で述べられている「情報システム」が、具体的にどの種のシステムを指すのかが記述されていないため、該当するシステムを開発しているものが、指針に該当しているかどうかを判断できないものになっている。移行指針の影響を受ける分野を具体的に示すには、例えば、Webブラウザ等のユーザ環境のシステム、オペレーティングシステム、組み込み機器、httpsを使ったサーバシステム、証明書発行を行う認証局システム、電子署名を扱うアプリケーション、その他の証明書検証サーバシステム等の記述が必要だと考えられる。これらの中には、技術仕様および市場の観点で、移行に必ず一定以上の時間がかかるものがあるため、少なくとも技術仕様の観点で移行が可能であることが確認されたスケジュールを提示し、該当するシステムを開発するものが、その他の要素について具体的に移行策を検討できるよう、移行指針の修正をお願いしたい。指針自体は暗号アルゴリズムの移行を目指しているのだが、内容は電子署名を強く意識したものとなっている。しかし、SHA-1は電子署名以外でもシステムの中で利用されており、移行の対象となるハッシュ関数の用途についても検討し移行の対応計画に含めることを指針に加えるほうが良いと考える。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	ご指摘のように、ハッシュ関数の用途は、電子署名以外にも様々あり、用途によっては相互運用性の観点からの検討が必要がないものもあると承知しており、暗号アルゴリズムの用途に応じた対応が必要と考えております。このため、政府機関全体の相互運用性の確保が必要なものである「ウ ア及びイ以外の情報システム」については、指針案においては、各府省庁が、それぞれが保有する情報システムの暗号アルゴリズムの用途に応じて対応を検討することとしており、「(2) 計画等の策定 ア」にあるように、当該検討を2008年度中にとりまとめるとしてあります。
3 内容 (2) 計画等の策定 イ	既に発行済みの電子署名付き文書ファイルについては、その電子署名の検証可能性を延長しデータの完全性を確保するためタイムスタンプを付与し、長期署名フォーマットに準拠して変換することを推奨する。 【財団法人 日本データ通信協会 タイムビジネス協議会】	今回の指針に従って決定すべき具体的な技術要件については、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。
3 内容 (3) スケジュール イ	RSA1024からRSA2048への移行の考え方は概ね正しいと考える。また、RSA2048について、GPKIの相互運用性仕様書では、RSA2048までの検証を要求しており、現時点でも検証は、可能なはずである。しかし、SHA-1からSHA-256への移行自体は正しいと考えられるが、実際の脅威となるまでの時間の推定は、「電子文書への署名」と「証明書の署名」では大きく異なるはずである。このため、一律にSHA-1の使用停止時期を決めるのは間違っていると考え、もし一律にSHA-1の使用停止時期を決めるのであれば、その根拠を明確にするようお願いしたい。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	SHA-1については、暗号研究の進展により、急激に安全性が低下する可能性があり、その危険性が指摘されています。一般に証明書の有効期間は一定期間保証されているものですので、SHA-256に情報システムが対応した後も、従来のSHA-1の利用停止時期を決めずに運用を続けた場合、急激な安全性の低下が発生した場合の対応が困難なことは明白なので、関係機関の状況を踏まえて適切な時期に利用を停止することは適切だと認識しております。 なお、これらの具体的なスケジュールについては、2008年度に詳細に検討することとしてあります。

該当箇所	御意見の概要	御意見に対する考え方
3 内容 (3) スケジュール イ	SHA-1の新たな暗号アルゴリズムへの切替時期並びに使用停止時期について、ハッシュアルゴリズムの危殆化は、「衝突困難性」に起因するものであり、その脅威については、エンドエンティティ署名に限定していることから、エンドエンティティで行う署名システムのみ、SHA-2対応に移行することを推奨する。 【財団法人 日本データ通信協会 タイムビジネス協議会】	今回の指針に従って決定すべき具体的な技術要件については、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。
3 内容 (3) スケジュール エ	NPO JNSAでは、2002年のIPAの公募の「電子政府情報セキュリティ相互運用支援技術の開発」に応募し採択され、この中で「GPKI 相互運用フレームワーク」を開発しオープンソースとして公開することにより、相互運用性のテスト環境を誰もが利用できるものとなっている。本指針にある検証環境の整備に関しても、同様なテストツールを提供し、誰でもこの検証環境が利用できる形態で提供されるようお願いしたい。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	今回の指針に従って決定すべき検証環境については、来年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。
その他	暗号技術検討会の報告書等では、RSA1024bitが解読可能になる時期については根拠が示されているが、SHA-1に関しては、現実的な脅威となる訳ではないコリジョン攻撃が可能になる推定のみが示されているのみであり、電子証明書に対する現実的な脅威になる可能性があるSecond-Pre-Image攻撃(第二原像計算攻撃)が可能になる計算量や、可能になると想定される時期は示されていない。こうした根拠が示されるべきではないか。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	電子署名の安全性に関しては、電子署名者による否認を防止できるレベルの信頼性を技術的に確保する必要があるため、第二原像計算攻撃による脅威のみならず、衝突計算攻撃による脅威も含めて想定する必要があると考えております。なお、今のところ、SHA-1の第二原像計算困難性について、現実的な脅威となるような攻撃手法は報告されておらず、その一方で、暗号技術検討会の下に設けられた暗号技術監視委員会からは、「SHA-1の安全性に関する見解」(平成18年6月)が示されており、その中で、「SHA-1を長期間にわたって利用する電子署名やタイムスタンプなどは、近い将来にSHA-1の衝突発見が現実的な問題に発展する可能性」が指摘され、「電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規(更新を含む)に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、SHA-256ビット以上のハッシュ関数の使用を薦める」という見解が示されております。このため、政府としては、暗号アルゴリズムの安全性の低下が現実的な問題となる前に、相互運用性の確保及び安全な暗号利用を推進する観点から、今回、SHA-1からSHA-256への移行を含む移行指針を策定することとしたものです。
その他	政府認証基盤(GPKI)の鍵更新は、最長5年のエンドエンティティの証明書発行することを想定した鍵管理のライフサイクルを想定していることと推測され、また、自己署名証明書は10年の有効期間で発行されている。利用するハードウェアに関しても住民基本台帳ICカードのように10年の有効期限を持ったものがある。こうしたことから移行に長い時間がかかることが想定されるが、今回の移行指針の提示は、あまりにも遅すぎるのではないかと、移行指針が提示自体は、遅すぎると考えるが、移行のスケジュールに関しては、十分に検討をお願いします。現状、電子署名は、それほど普及している訳ではない。無理な移行スケジュールは、適切に電子署名が利用されるべき場面においても、電子署名が利用されなくなる可能性も高いと考えるため、電子署名が使われなくなるため問題も無くなるといった本末転倒な結果にならないよう十二分に検討をお願いします。 【特定非営利活動法人 日本ネットワークセキュリティ協会 PKI相互運用技術WG】	今回の指針に従って決定すべき具体的なスケジュールについては、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。
その他	今回対象となっているのは、SHA-1およびRSA1024に関しての移行ということだが、それらの暗号アルゴリズムが電子政府の「どこで、なんのために、どのように」使われているかについて網羅されているか？同じ暗号アルゴリズムであっても、その使用用途によって特定の脆弱性が与える影響は様々であり、例えばその脆弱性が単に解読時間の短縮によるものであれば、相対的に有効期限が短い使用用途について与える影響は最小限である。また、移行必要とされる場合でも、それに要する期間や負荷については様々なケースがあると考え、今回の方針は、俯瞰的な視点において出されたものかとは思いますが、電子政府における暗号の使われ方に関する網羅的な調査をぜひ実施して頂きたい。 【日本クロストラスト株式会社】	今回の指針に従って決定すべき具体的な対応等については、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。なお、本指針案では、「3(1) 情報システムの設計要件」において、「情報システムにおける暗号アルゴリズムの用途を踏まえつつ、それぞれの情報システムにおいて、以下のように設計を行う。」とあるように、用途に応じた対応を検討することとしております。
その他	「政府機関の情報システム」というのがどこまでの範囲を含むものかは明確ではないが、CRYPTRECから平成15年に出されている「電子政府推奨暗号リスト」にSSLについての言及があること、また、「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)」でも5.3.3に「ウェブサーバの正当性を保証するために電子証明書を利用すること」とあることから、SSL/TLSもその対象に含まれるものと推察する。SSL/TLSにおいてはRSA2048への移行は既に始まっているものの、SHA-211については手がついていない、SSL/TLSはインターネット上で最も広く使われている暗号化手段であると言っても過言ではないかと思うが、その移行に関して今回の指針ではどのように取り扱われるのか。 【日本クロストラスト株式会社】	今回の指針に従って決定すべき具体的な対応等については、2008年度に詳細に検討するため、ご指摘については、今後の検討の参考とさせていただきます。なお、本指針案では、「3(1) 情報システムの設計要件」において、「情報システムにおける暗号アルゴリズムの用途を踏まえつつ、それぞれの情報システムにおいて、以下のように設計を行う。」とあるように、用途に応じた対応を検討することとしております。
その他	RSA1024やSHA-1だけでなく、基本的に全ての暗号アルゴリズムは将来的にどこかの時点でその安全性に疑問が生じることをあらかじめ考慮することが必要であると思う。SHA-2とRSA2048への移行が2013年に完了したとして、その次の移行時期に関する検討は進んでいるか？米NISTでは次世代ハッシュアルゴリズムへの公募を開始しており、2011年末には採用アルゴリズムの発表が予定されている。またRSA2048についても、専門家からは2020年代半ばにはその安全性に疑問符がつくであろうという予測が出ている。特にPKI認証局は数十年の運用を前提としている場合が多く、また、移行に長い期間を必要とすることから、そこに採用されるべきアルゴリズムの選定とスケジュールには特に注意が必要であると考え、 【日本クロストラスト株式会社】	本指針案は、SHA-1及びRSA1024の移行指針であるため、ご指摘については、今後の参考とさせていただきます。なお、今回の指針案における対応後、将来的には、再度暗号アルゴリズムの移行が行われることとなることについては承知しておりますので、その検討は今回のような暗号アルゴリズムの安全性の低下への対応とは別に、今後あらかじめ検討されるべきものと考えております。