資料7－3

オンライン手続におけるリスク評価及び電子署名・認証ガイドライン(案)についての パブリックコメント提出意見及び回答

平成22年8月31日

内閣官房情報セキュリティセンター

1. 意見募集の概要

オンライン手続におけるリスク評価及び電子署名・認証ガイドライン(案)に関して、以下のとおりパブリックコメントの募集を実施した。
○募集期間：平成22年2月2日（火）～平成22年3月3日（水）
○告知方法：電子政府の窓口（e-GOV）及びIT戦略本部ホームページ、情報セキュリティセンターホームページ
○意見提出方法：電子メール、FAX、郵送のいずれか

2. 提出された意見数

意見提出者数： 17件（個人4、団体13）
意見提出数： 116件

3. 提出された意見の概要及びそれに対する考え方について

整理番号	個人／団体	ガイドライン（案）における項番	ご意見（概要）	考え方
1	団体	1.3.	本ガイドラインの対象範囲が局所的・限定的ではないか。	本ガイドラインは「国民・企業と政府の間の申請・届出等のオンライン手続」をすべて対象としております。
2	団体	2.	用語定義を精緻化して欲しい。	ご指摘を踏まえ、修正しました。詳細は、「2. 用語定義」をご確認ください。
3	団体	3.1.	本ガイドラインで対象外となる攻撃の具体例を記載して欲しい。	本ガイドラインは、認証方式の有効性とは関連性がない脅威をリスク評価の対象外としていますが、「例えば、～」以下及び図3-1で説明しています。
4	団体	3.2.	本ガイドラインの対象となる脅威行動の抽出の理由をより明確にして欲しい。	ご指摘を踏まえ、「3.2. オンライン手続に関わる脅威」を修正しました。
5	団体	3.3.	「特高」という言葉は、別の意味を持つので置き換えた方が良いのではないか。	レベルの影響度を表す指標の一つとして「特高」を定義しているにすぎません。
6	団体	3.4.	取り扱うリスクの種類について、今後、他の4項目についても評価対象に加えることが好ましい。	当ガイドラインでは、「国民・企業と政府の間の申請・届出等のオンライン手続」を対象としており、当該手続においては、「金銭的被害」及び「機微情報の漏えい」が主たるリスクと認識しています。他のリスクについては総合的にリスク影響度を導出する際に勘案することとしています。
7	団体	3.5.	重点47手続が何を指すのか付録等で示して欲しい。また、なぜ重点手続き71から、電子署名を要する47のみ選んでガイドラインの対象としているのか、それをもってオンライン手続のガイドライン作成の根拠とすることの妥当性を示して欲しい。	・本ガイドラインは「国民・企業と政府の間の申請・届出等のオンライン手続」をすべて対象としております。 ・重点手続については、「オンライン利用拡大行動計画」（http://www.kantei.go.jp/jp/singi/it2/kettei/080916honbun.pdf）をご参照下さい。 ・ガイドライン策定にあたっては、重点手続のうち、電子署名を要する47手続を中心にリスク評価方法を検討しました。
8	団体	3.5.1.	金銭的被害の場合だけ、申請の厳格さとの2次元評価になっている理由がよくわからないので明示して欲しい。	リスク評価のあたっては、種々の要素を勘案する必要があると考えられますが、金銭的被害のリスクについては、ガイドラインにあげている2つの評価軸が一般的なリスク評価手法からしても適当と判断しました。
9	団体	3.5.1.	金銭的損害のリスク評価において、「申請等に係る厳格さ」を評価軸に採用することは、簡易な方法として妥当性があるものと理解できるが、中長期的には見直しを含めた検討が必要になるものと考える。この点について、注記などを行うことが適切ではないか。	本ガイドラインで導出された、妥当性は継続的に確認することとし、必要に応じリスク評価等の見直しを行うこととしておりますので、頂いたご意見は、今後の検討の参考とさせて頂きます。
10	団体	3.5.1.1.	事案がもたらす被害規模については、直接的な被害のみを取扱うのではなく、補償や補填、システム復旧に係るコスト等の間接的な被害によるものも対象にするべき。	間接的な被害について、どのうように評価するかを一意的に定めることは困難であると判断し、本ガイドラインでは、直接的な被害のみ具体的に記載しています。間接的な被害は、対象外とするのではなく、総合的なリスク評価で勘案することとしています。
11	団体	3.5.1.1.	繰り返し発生する申請などは、その総額の影響度合いを適切にリスク評価に組み入れる必要があると考える。	本ガイドラインにおいては、当該手続き1件あたりによることを基本としています。しかしながら、同様の手続きを複数回行うなど被害額が積み上がり配慮が必要な場合などは、総合的なリスク評価で勘案することとしています。
12	団体	3.5.1.2.	3.5.1.2の申請等に係る厳格さとA.3.2の登録の保証レベルが対応していないのではないか。	3.5.1.2と「手続全体に求められる厳格さの評価尺度」、A.3.2は「認証対象者の登録に求められる厳格さの基準」を定義したものであり目的も範囲も異なるため、必ずしも一致するものではないと考えます。
13	団体	表 3-5	レベル「特高」の申請等に係る厳格さの程度において、“主体以外が保有するデータベースと照合を実施”とあるが、目的外使用や個人情報保護の関連で主体以外が所有するデータベースの要件を明確にすることが必要ではないか。	本ガイドラインでは、申請等にかかる厳格さの機能についてレベル分けしています。目的外使用や個人情報保護などへの配慮は、個々の実際のデータ利用にあたって運用を整理することとなります。
14	団体	表 3-6	情報の重要度のレベルの違いが不鮮明と感じられるため、より明確な記述をお願いしたい。	本ガイドラインで導出された、妥当性は継続的に確認することとし、頂いたご意見は、今後の検討の参考とさせて頂きます。
15	団体	3.5.4.	代理人が介在することによってリスクは大きくなることが既定の事実と考えられているように読める部分があるが、その理解でよいか。	代理人が介在することによるリスクの大小は、場面ごとに異なるものと考えております。しかしながら、各国民による手続に比べ、代理人が複数あるいは多数の手続きを行うとの特性からなりすましによる影響の大きさなどリスクが顕在化した場合の影響度は大きいと考えられ、このような申請者等の特性を考慮すべきであると考えております。

整理番号	個人／団体	ガイドライン（案）における項番	ご意見（概要）	考え方
16	団体	3.5.4.	総合的リスク評価の導出方法として、「金銭的損害に係るリスクの影響度」と「機微情報の漏えいに係るリスクの影響度」等の評価結果が異なった場合には、高いレベルのリスク評価値を採用することを「原則」とし明記することが適切ではないか。	本ガイドラインでは、総合的なリスク影響度を導出するにあたり、相応のリスクの影響度を導出するのは当然ですが、その際、ユーザーの利便等にも配慮の上、リスク種類ごとの回復可能性等を考慮し、リスクの影響度の評価値の最も高いレベルを機械的に採用するのではなく、十分に検討することを求めています。
17	団体	4.	「・・・セキュリティ確保策として電子署名・認証の適用を検討する際を想定する。」とあるが、電子署名の用途とセキュリティ確保策との関係が明確でないので、関係の説明が必要ではないか。	対象となる電子政府システムが、セキュリティ確保策として電子署名・認証の機能を必要とするかは、当該システムの特性によるものと考えております。説明については、A.2.2.をご覧ください。
18	団体	図4-1	図4-1ではリスク評価および保証レベル導出はシステム開発・運用当事者である各府省が行い、結果をCIO連絡会議等へ報告することになっているが、当事者府省の内部で閉じた検証をするのではなく、開かれた検証によってシステム・セキュリティの透明性を確保する必要があるのではないか。	各府省庁においては専門的知見を有するCIO補佐官から総合的な助言を受けるとともに、各省庁のCIO等が参加するCIO連絡会議等に報告することとなっています。 これにより、府省庁の内部、外部で検証されるためシステム・セキュリティの透明性を確保できると考えています。
19	団体	A.3.2.	システムへの利用者の登録(複数人による運用)など運用に関してガイドラインとしての基準を示す必要があるのではないか。 また、登録に関する申請書類の保管管理などの運用に関してガイドラインとしての基準を示す必要があるのではないか。	本ガイドラインでは、政府機関において特に重要度が高いと考えられる基本的な対策基準を策定しています。したがって、民間分野も含めた多様なサービスを想定した対策基準の網羅性の確保は必ずしも行わず、ご指摘頂いた点等については事業者ごとに検討頂くものとしました。
20	団体	表 A.3-3	対策基準に「重複登録ではないことを確認する。」とあるが、この内容は、基準としてレベル4に組み込むことが適切か疑問に感じる。	A.1の参考（P.27）に記載の通り、保証レベル4の用途は極めて重要性の高い業務を想定したものであり、業務の主体者の特定には厳密性が求められます。同一人物が重複登録により複数のIDを取得することは、認証による主体者の同一性の確認を妨げる恐れががあるため、許容すべきではないと考えます。
21	団体	表 A.3-3、表 A.3-4 表 A.3-6、表 A.3-7 表 A.3-9、表 A.3-11 A.4.2.、A.5.6.	対策基準等について、これらの具体的な内容（要件）を明確にするために、実例を追加して欲しい。	ご指摘を踏まえ、修正しました。詳細は、ガイドライン本体をご確認ください。
22	団体	表 A.3-4	遠隔の場合の保証レベルの要件が対面よりも弱くなってしまっているので、整合させるべきではないか。	ご指摘を踏まえ、表A.3-4の該当箇所の補足説明を追記しました。
23	団体	表 A.3-4	クレジットカード番号を認証の手段とする場合には、カード会社へ、カードの有効性の問合せを行うことを意図しているのか。	ご指摘頂きました表A.3-4の例示は、登録申請にあたって決済行為を伴う場合に、結果として他機関の登録情報に基づく対象者の存在確認の効果が得られることを想定したものであり、登録時の本人確認のみのためにクレジットカード番号を用いることを必ずしも意図しておりません。ご指摘を踏まえ、表A.3-4の該当箇所の補足説明を追記しました。
24	団体	表 A.3-5	(a)表中に「漏えい」を追加するとともに、その対策例を記載して欲しい。	ご指摘を踏まえ、表A.3-5を修正しました。
25	団体	表 A.3-6、表 A.3-7 表 A.3-9、表 A.3-10 表 A.3-11、表 A.3-12 表 A.4-3、A.5.6.	対策基準等について、誤解を生じないように文言を精緻化して欲しい。	ご指摘を踏まえ、修正しました。詳細は、ガイドライン本体をご確認ください。
26	個人	A.3.4.	電子政府を使う国民を対象とするガイドラインであるなら、パスワードに関する考察と記述をもっと掘り下げ、パスワード自体の安全基準や推奨すべき形態に言及するべき。	適切なID／PWの活用は安全性と利便性、経済性のバランスの観点から重要であると考えることから、今後の検討に向けての参考にさせていただきます。
27	団体	A.3.4.	生体特徴点トークンもトークンの1つとして追記して欲しい。	セキュリティ分科会報告書の「3.3.1.1 生体認証」においても記載しているとおり、生体特徴点トークンについては、現状では、誤受入率・誤拒否率といった用語の統一だけでなく、セキュリティの評価尺度の確立、そして、同一基準でのセキュリティの測定・評価が難しいため、今後の検討に向けての参考にさせていただきます。
28	団体	A.3.4.	アクセス方法の多様化や端末の多様化の進展に鑑み、屋外環境・モバイル環境での利用シーンを前提にリスク評価を図ることが望ましい。	屋外環境・モバイル環境での利用シーンを前提としたリスク評価については、今後の検討に向けての参考にさせていただきます。
29	団体	表 A.3-9	数値データ、2^{-10}（1024分の1）、および2^{-14}（16384分の1）の根拠を示していただきたい。	A.1に記載の通り、本ガイドラインの対策基準は、ご指摘の箇所を含めNIST SP 800-63を参考にして策定されています。
30	団体	表 A.3-10	4桁暗証番号はレベル1にも達せず、使うべきではないのではないか。	ご指摘の箇所の対策基準は、推測確率により条件が定められております。数字（10種の文字）のみによる 4桁のパスワード（暗証番号）の推測確率は、レベル1の条件を満たすことができません。 ただし、ASCII の印字可能文字（94種の文字）を用いる場合には4桁であってもレベル1の条件を満たすと推定されます。また、レベル1の用途で、数字のみをパスワードに用いる場合、5桁以上が必要となります。 なお、パスワード長とエントロピーの関係に関しては、本ガイドラインにて参考とした NIST SP 800-63 の付録に詳しい解説が掲載されています。
31	個人	A.4.2.	現在、電子署名を必要とする47のオンライン手続及び民間認証局の電子証明書がどの保証レベルに該当するのか明示して欲しい。	「4. リスク評価に基づく認証方式の選択等の実施」に記載のとおり、本ガイドラインの適用時期については、「各府省が当該オンライン手続にかかる電子政府システムの新規構築又は改修を行う際の計画策定や要件定義等の企画段階などでセキュリティ確保策として電子署名・認証の適用を検討する際」であり、現時点でのオンライン手続き及び民間認証局の電子証明書は保証レベル導出の対象としていません。
32	団体	表 A.4-3、表 A.4-4	保証レベル4の対応で、ハードウェアトークンをオプションとして欲しい。	A.1の参考（P.27）に記載の通り、保証レベル4は、例えば、政府機関において極めて重要性の高い業務を想定したものであり、耐タンパ性を有するハードウェアトークンの利用が適切であると考えます。
33	団体	表 A.4-3、表 A.4-4	保証レベル3に対応する電子証明書は、新たな認定認証業務の基準作成を想定されているのか、認定認証業務以外の民間認証局の電子証明書を用いることを想定されているのか教えていただきたい。また、新たな認定認証業務の基準作成を想定されている場合、早急にスコープを示して欲しい。	本ガイドラインの策定については、新たな認定認証業務の基準作成を想定しているものではございません。

整理番号	個人／団体	ガイドライン（案）における項番	ご意見（概要）	考え方
34	団体	表 A.4-3、表 A.4-4	署名等プロセスの対策基準、署名等プロセスの保証レベルにおいて、保証レベル3と保証レベル4のケースが想定されています。保証レベル4の耐タンパ性を備えた電子証明書は、署名等プロセスで使用する電子証明書が唯一の存在であることを保証する手段であり、その利用用途に応じて保証レベル3と明確に区別できるような手段を明示して欲しい。	ご指摘の点については、今後の検討に向けての参考にさせていただきます。
35	団体	A.5.4.	本ガイドライン付録において可能性として示されている『複数のサービス間で共用する認証連携基盤の導入』について民間システムとも連携する方式で早急に推進して欲しい。	ご指摘の点については、今後の検討に向けての参考にさせていただきます。
36	団体	A.5.4.	A.5.4.の記述をみると、ユーザビリティ的に「セキュリティの大は小を兼ねる」かのごとくに見える。しかし、ユーザビリティなどを考えると、これは明らかに正しくないので、より正確な記述に改めて欲しい。	「A.5.1. 対策基準の適用の考え方」において、認証方式の強度とコスト及び利便性が一般的にトレードオフの関係にあることを指摘し、セキュリティ上の理由でむやみに上位レベルの対策基準を採用することは適切ではないと記載しております。
37	団体	A.5.5.	証跡や署名を施した文書を、安全に長期間の利用・保存するための長期署名等の技術についても検討して欲しい。	ご指摘の点については、今後の検討に向けての参考にさせていただきます。
38	個人	A5.5.	オンライン手続きにおける認証と、手続記録の真正性維持とは別の観点からの検討が必要ではないか。	真正性確保のための証跡管理手法に関するご指摘については、今後の検討に向けての参考にさせていただきます。
39	団体	全体	「認証方式の保証レベルに係る対策基準」は、付録という位置づけではなく、ガイドラインの本文をなすべき項目ではないか。	ご指摘の点については、今後の検討に向けての参考にさせていただきます。
40	団体	全体	電子署名に係る基準については、原案において、未整理な事項が多数存在するように感じられる。例えば、少なくとも、以下のような項目の整理を行うことが、国民の混乱を防ぐ上で重要と考える。 (1) 電子署名法第3条に規定された電子署名との関係 (2) 認証と電子署名との本質的な違いの説明と、これに対する対応の方針 （※一般に、電子署名には本人の「意思」が含められていると考えられる） (3) 電子署名のプロセスについてのさらなる分析と要件定義 (4) 公的個人認証サービスにより発行された電子証明書との関係 (5) 商業登記に基づく認証局（電子認証登記所）より発行された電子証明書との関係 上記のうち(1)(3)については、関連する民間サービスが複数存在することから、特に慎重な議論を行い納得性の高いガイドラインを作成して欲しい。 このような現状を省み、電子署名については、現時点での拙速な結論とせず、今後のさらなる議論の継続をお願いしたい。	ご指摘の点については、今後の検討に向けての参考にさせていただきます。
41	個人	全体	法制度等による本人確認手続きへの信頼に基づく考えを考慮するべき。	今回はオンライン手続きを対象に検討したものですが、報告書の今後の検討課題のなかで、本人確認に関する横断的な制度設計の必要性を指摘しております。
42	個人	その他	不動産登記の（書面で通知された）登記識別情報の目隠しシールが剥がれず、12桁の記号を判読することができない問題があり、法務省は、法律上の根拠もなく再通知することを検討しているが、違法な対応策を検討するのではなく、電子署名の有効利用を検討すべきである。 不動産登記のオンライン申請は、特例方式の場合であっても申請人本人の電子署名を要件として、登記識別情報（12桁の記号）の提供は不要とする申請方法を提案する。	ご意見は、今後の検討の参考とさせて頂くとともに、制度を所管している法務省に連絡させていただききます。
43	個人	その他	実質書面申請の特例方式をオンライン申請と称して、登録免許税を年間100億円も無駄に軽減するのではなく、公的個人認証カードの無料配布等、電子証明書を普及させるための施策を実施するべき。	ご指摘の点については、今後の検討に向けての参考にさせていただきます。
44	団体	その他	リスク評価をしセキュリティを重視することは必要ですが、電子政府の利活用率が向上するまでの間は、ユーザビリティを最優先し、利用者目線で構築するオンライン手続きにして欲しい。	セキュリティと利便性とコストはトレードオフの関係にあるため、利便性のみを優先することはできませんが、利用者目線で構築するために考慮すべき要件をガイドラインに盛り込んでおります。

※本表のご意見（概要）は、受け付けたパブリックコメントを元に、内閣官房情報セキュリティセンターにおいて要約したものです。