



オンライン手続における リスク評価及び電子署名・認証ガイドラインの概要

2010年8月31日

内閣官房情報セキュリティセンター(NISC)

1. ガイドラインの概要

- 我が国の電子政府における認証方式の設計にあたり活用可能な「ものさし」を確立することを目的として策定。
- ガイドラインは、対象となる電子手続に関するリスク評価手法とこの手法により導出される「リスクの影響度」、影響度に応じた認証方式の「保証レベル」の導出、各保証レベルに求められる対策基準を規定。

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

電子政府の手続に関わるリスク評価手法、リスクの影響度と対応する保証レベルの考え方



【付録】電子署名・認証の保証レベルに係る対策基準

保証レベルに見合う登録、発行管理、トークン、認証プロトコルの対策基準の考え方



2. ガイドラインの概要(リスクの影響度と保証レベル)

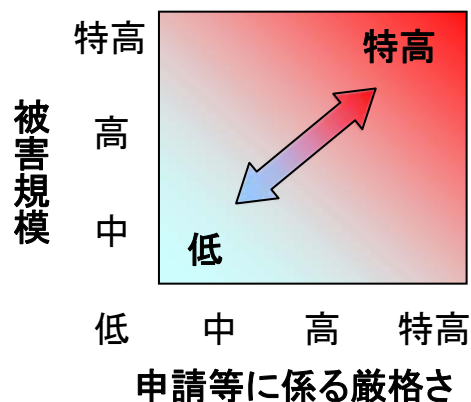
● リスクの影響度の定義

「リスク影響度」を「特高」「高」「中」「低」の4段階に定義。

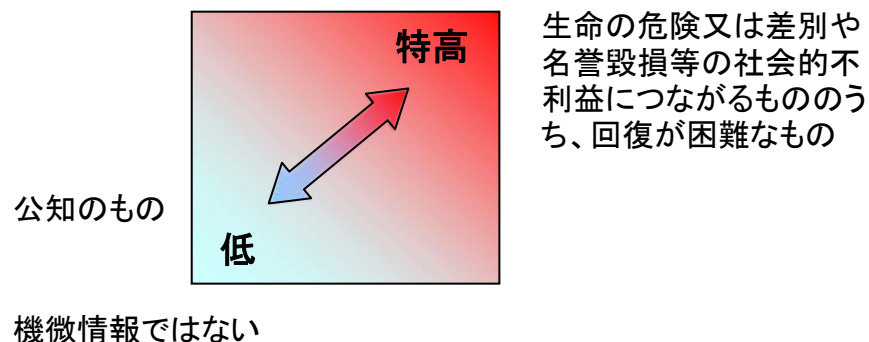
● リスクの評価

いくつかのリスクが想定されるが、オンライン申請等の電子政府サービスにおいては、「機微情報の漏えい」と「金銭的被害」の2つのリスクが主に発生する可能性があり、この2つのリスクについて影響度の導出方法を定義。

【金銭的損害に係るリスクの影響度】



【機微情報の漏えいに係るリスクの影響度】



● 総合的リスク評価の導出

「総合的なリスクの影響度」の導出においては、金銭的損害に係るリスク、機微情報の漏えいに係るリスクの他、二次的被害、申請者等の特性、回復可能性など、全ての要素を考慮の上、手続固有の特性を踏まえ導出する。

● リスクの影響度による保証レベルの導出

「総合的なリスクの影響度」から「保証レベル」を導出する。この保証レベルに応じた「対策基準」を参照することにより、当該手続きのリスクの影響度に見合った合理的な認証方式の選択が可能となる。

| 総合的なリスクの影響度 | 保証レベル |
|-------------|-------|
| 特高 | レベル4 |
| 高 | レベル3 |
| 中 | レベル2 |
| 低 | レベル1 |

3. ガイドラインの概要(対策基準)

- 各保証レベルに求められる具体的な対応基準を、4つの評価軸ごとに規定。
- 対策基準の適用の考え方(※1※2)など、基準実現のための配慮事項についても規定。

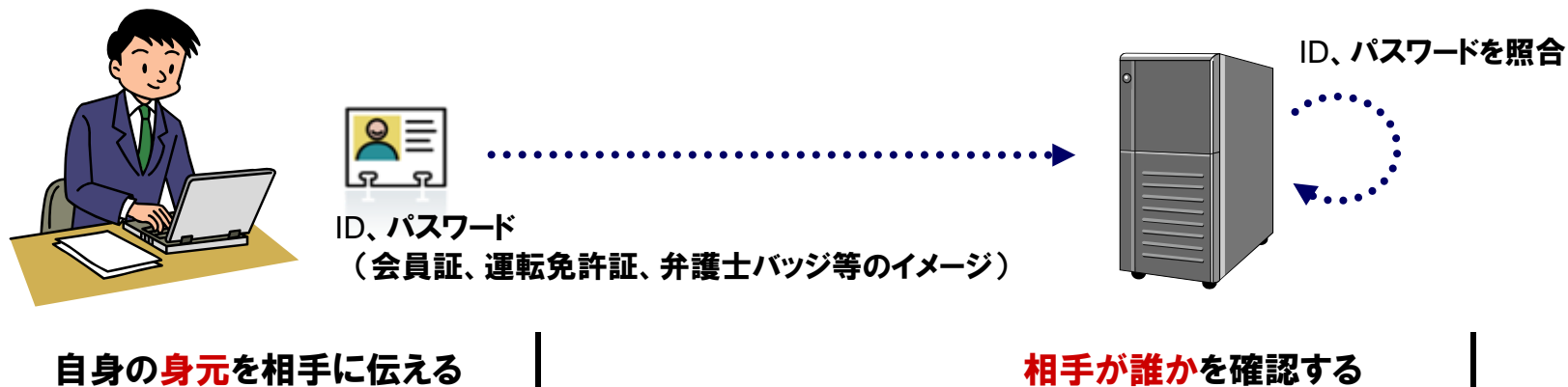
<主な対策基準>

| 保証レベル | 登録 | 発行・管理 | トークン | 認証プロセス | 署名等プロセス |
|-------|--|---|---|--|--|
| レベル4 | (窓口) ・ 写真付き身分証明1種の提示 ・ 申請情報の台帳照合 ・ 重複登録ではないことの確認 | ・ 手渡し、本人限定受取郵便、によるトークン発行 | ・ レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること | ・ レベル3と同等の基準 | ・ 電子政府推奨暗号リストに記載の署名方式 ・ 電子署名用の証明書の用途は電子署名限定 |
| レベル3 | (窓口) ・ 写真付き身分証明1種(or他2種)の提示 ・ 申請情報の台帳(又は公的証明書)照合(郵送 or オンライン) ・ 申請書に対する電子署名 ・ 申請情報の台帳(又は公的証明書)照合 | ・ レベル4の方法に加え、書留郵便、書留郵便+ダウンロード、電子署名+ダウンロード、によるトークン発行 | ・ レベル2の基準に加え、複数の認証要素を利用すること | ・ レベル2と同等の基準に加え、フィッシングの脅威に対する耐性 | ・ 電子政府推奨暗号リストに記載の署名方式 |
| レベル2 | (窓口) ・ 写真付き身分証明1種(or他2種)の提示(郵送 or オンライン) ・ 申請情報に他機関の登録情報(クレジットカード番号等)を含めて申告 | ・ レベル3の方法に加え、分割配付(一方を郵送)、メール通知後のダウンロード、によるトークン発行 | ・ 認証情報の推測確率が16384分の1未満であること | ・ レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性 | |
| レベル1 | (窓口 or 郵送 or オンライン) ・ 身元確認は不要 ・ メールアドレスの到達確認 | ・ レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行 | ・ 認証情報の推測確率が1024分の1未満であること | ・ オンライン上の推測、リプレイ攻撃の脅威に対する耐性 | |

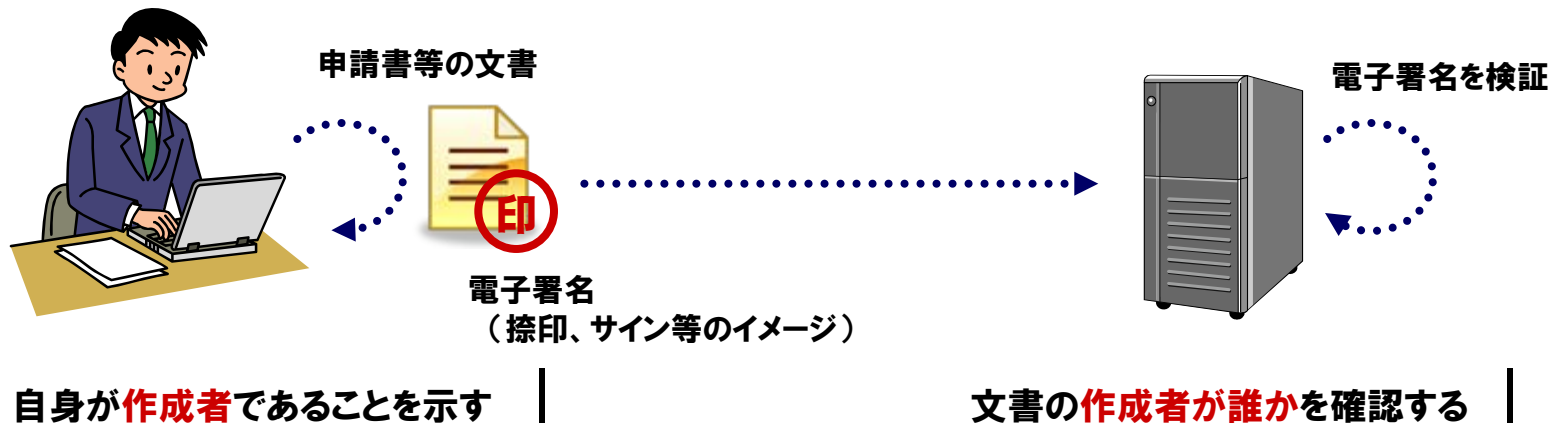
※1 上位基準の採用: 認証方式の強度とコスト及び利便性は一般的にトレードオフの関係にあり、コストや利便性等の多様な観点による総合的な判断が必要となる。

※2 代替基準の採用: ガイドラインの対策基準は絶対的なものではなく、同等の代替基準であれば他の対応策による代替が許容される。

認証（アクセス元の利用者の本人確認を行うこと）



電子署名（文書の作成者の確認を可能とする情報、またはそのような情報を文書に付与する行為のこと）



- 「リスク評価を実施」、「保証レベルを導出」のプロセスにおいて、個別手続き毎の保証レベル、対策基準の検討。
- 「対策基準の選択」のプロセスにおいて、その他のリスク削減方策の採用や、保証レベルが異なる複数の手続によって構成されるサービスの場合におけるユーザの利便性、サービス提供者側とユーザ側を合わせたライフサイクルコストの観点等から見て、総合的に判断して最終的な対策を決定。
- 選択された対策やリスク評価について、各府省は、それらの適切さを確保するために情報セキュリティ対策推進会議等の場において専門的知見を有する者からの助言等を受け、決定するとともに、業務・システム最適化に係るものは、計画への反映状況について、CIO連絡会議等に報告するものとする。(※)
また、電子政府評価の一環として、必要に応じ各府省に対してガイドラインに基づく取組の報告を求め、評価等を行う。

(※)ここで、最適化計画への反映については、当該計画の改訂のタイミングとする。

