資料2－1

オンラインにおける行政手続の本人確認の手法に関するガイドラインについて

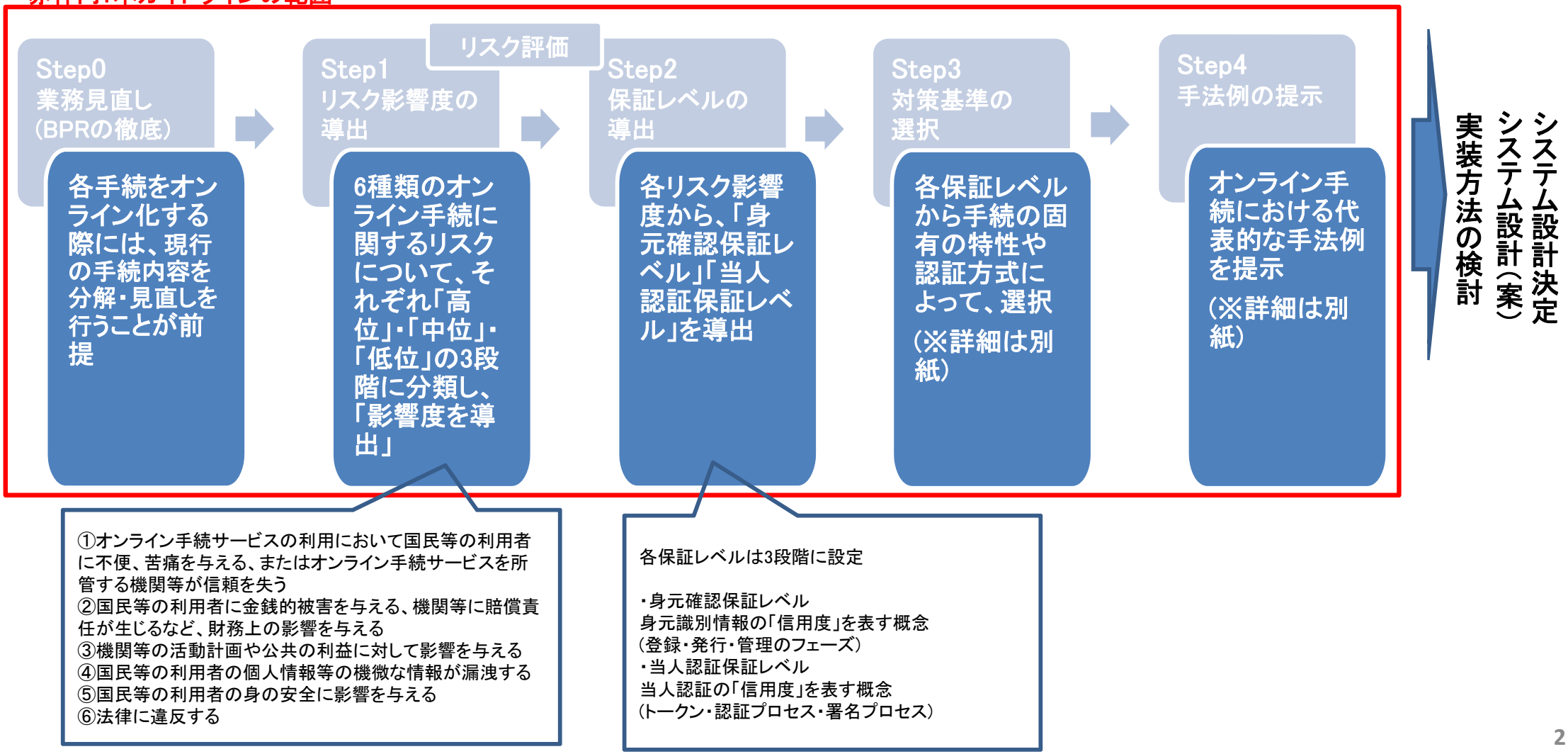
2019 年 3 月 5 日

内閣官房　情報通信技術(IT)総合戦略室

1. オンラインにおける行政手続の本人確認の手法に関するガイドラインの概要

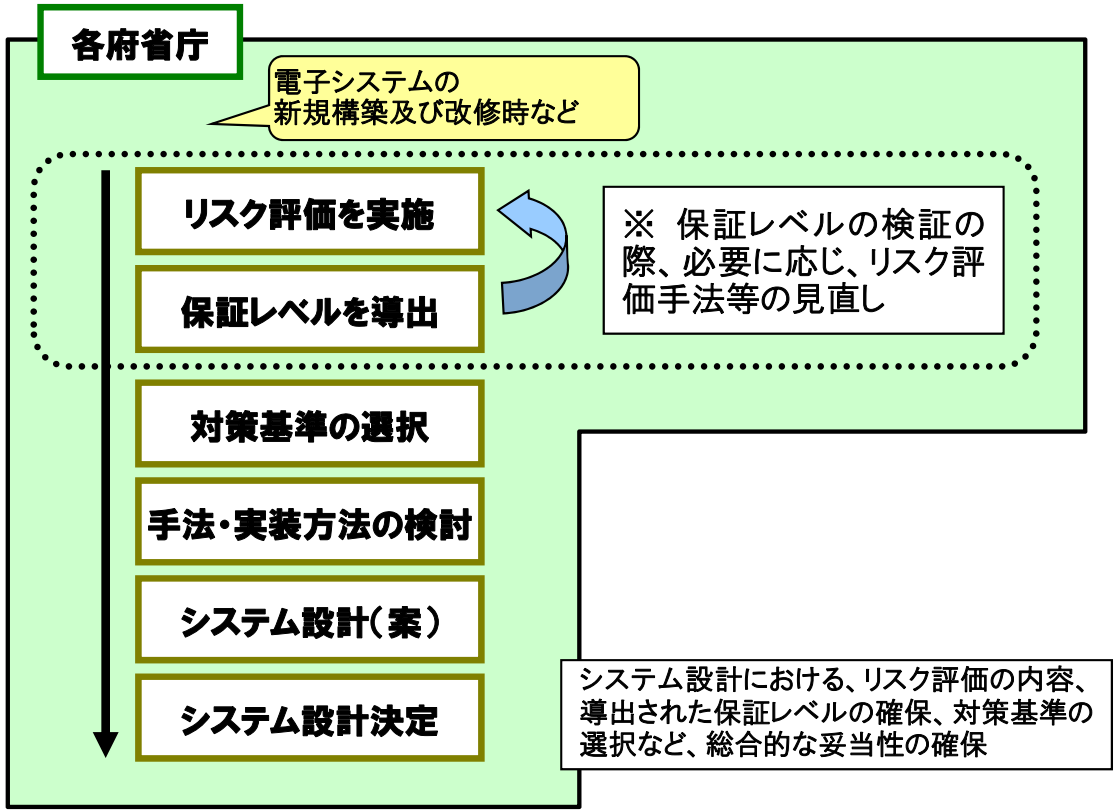
- 行政手続のオンライン化を進めるにあたり、デジタルによる認証方式を選定するうえでの考え方・手法例として策定。
- 本ガイドラインは、行政手続をオンライン化する際に考慮すべき、リスク評価手法とこの手法により導出される「リスクの影響度」、その影響度に応じた認証方式の「保証レベル」の導出、各保証レベルに求められる「対策基準」を規定している。
- Step1～3において、国際的に広く使われているNIST SP800-63-3を参考にガイドラインの策定を行った。

赤枠内：本ガイドラインの範囲



2.ガイドラインの活用方法

- 個別手続き毎に「リスク評価を実施」、「保証レベルを導出」を行い、保証レベル、対策基準の検討を行う。
- 「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ーの利便性、サービス提供者側とユーザー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。



セキュリティ対策及び利便性は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から総合的に判断する。

3.対策基準の概要　～ Step3

■ 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	身元確認		当人認証		
	登録(※3)	発行・管理(※4)	トークン	認証プロセス	署名等プロセス
レベル3	**(対面の場合)** ・公的な写真付き身分証明書1種の提示 ・申請情報の公的な台帳照会 ・重複登録ではないことの確認	・手渡しによるトークン発行 ※本人限定郵便基本型及びこれと同等の手段は対面として扱う	・レベル2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(※5)	・レベル2と同等の基準	・電子政府推奨暗号リストに記載の電子署名 ・電子署名用の証明書の用途は電子署名限定
レベル2	**(対面の場合)** ・公的な写真付き身分証明1種(または2種の提示) ・申請情報の台帳(又は公的証明書)の照合 **(郵送 又はオンラインの場合)** ・申請情報に対する電子署名(郵送の場合は署名又は捺印) ・申請情報の台帳(又は添付の公的証明書)照合	・レベル3の方法に加え、書留郵便＋ダウンロード、電子署名＋ダウンロード、携帯電話の番号検証＋ダウンロードによるトークン発行	・記憶された秘密、認証デバイス、生体認証の中から複数の認証要素を利用すること	・レベル1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電子署名
レベル1	**(対面、郵送又は オンラインの場合)** ・メールアドレスの到達確認 ※身元確認は不要	・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	・記憶された秘密、認証デバイス、生体認証の中から単一又は複数の認証要素を利用すること	・オンライン上の推測、リプレイ攻撃、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	

※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。
※3　各レベルで掲載事項のうち該当するものをすべて満たす。
※4　各レベルで掲載事項のいずれかを満たす必要がある。
※5　法律に基づき設置された団体等が、申請者の身元情報や資格を確認した上で発行する電子証明書に関するパスワード付きソフトウェアトークンについては、当該資格を所管する省庁によって有資格者本人に対する通知を行うことが可能であることを等を踏まえた追加的対策によりリスク軽減がなされたと評価される場合には、所管省庁の判断において、保証レベル2に対する認証方式の選択も可能と考えられる。

4-1.手法例（個人に係る行政手続） ～ Step4

①必要な保証レベル		②オンラインによる手法例		③実現できること・特徴
身元確認保証レベル	当人認証保証レベル			
レベル3 対面での身元確認	レベル3 耐タンパ性が確保されたハードウェアトークン	レベルA	・マイナンバーカード(公的個人認証：署名用電子証明書)による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード(公的個人認証：利用者証明用電子証明書)の耐タンパ性ハードウェアトークンによる当人認証を実施。 ・申請データに対するマイナンバーカード(公的個人認証：署名用電子署名証)による電子署名を付与 ※耐タンパ性ハードウェアトークンの例： － PIN+ICカード(マイナンバーカード)	・行政手続の対象者や行政手続を実施している者について、個人の基本4情報を毎回確認している。 ・マイナンバーカード(公的個人認証：署名用電子証明書)の機能により付与された電子署名を検証することにより、非常に高い信用度で「身元確認」を行っている。また、耐タンパ性を有したハードウェアトークンにより非常に高い信用度で「当人認証」を行っている。
レベル2 遠隔又は対面での身元確認	レベル2 複数の認証要素	レベルB	・マイナンバーカード(公的個人認証：署名用電子証明書)等による身元確認でアカウントを作成し、アカウント作成後はマイナンバーカード(公的個人認証：利用者証明用電子証明書)若しくはこれによることができない場合、その他の多要素認証による当人認証を実施。 ・マイナンバーカードによるオンランでの身元確認が行えない場合、対面での身分証明書等の確認や郵送した申込書(捺印付)、印鑑証明書、公的証明書(住民票等)等の確認によりアカウントを作成。 ・法人共通認証基盤における多要素認証の機能を利用する場合等、事業を行う個人についての押印及び印鑑証明書等の郵送による身元確認で、アカウント作成し、アカウントを作成後は多要素認証による当人認証の実施。 ※多要素認証の例： － ID・パスワード+二経路認証アプリ － ID・パスワード+ワンタイムパスワード生成アプリ － ID・パスワード+生体認証	・行政手続の対象者や行政手続を実施している者について、登録時に個人の基本4情報を確認し、認証プロセス時には、同一の個人であることを確認している。 ・登録時に相当程度の信用度のある「身元確認」を行い、マイナンバーカード(公的個人認証：利用者証明用証明書)等の多要素認証の機能を用いることで、相当程度の信用度で「当人認証」を行っている。 ・特に法人共通認証基盤においては、登録時に事業を行う個人を相当程度の信用度で「身元確認」を行い、多要素認証の機能を用いることで相当程度の信用度で「当人認証」を行っている。
レベル1 身元確認のない自己表明	レベル1 単一又は複数の認証要素	レベルC	・身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ・法人共通人認証基盤における単要素認証の機能を利用する場合等、身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施 ※単要素認証の例： － ID・パスワードのみ － 認証デバイスのみ － 生体認証のみ	・行政手続の対象者や行政手続を実施している者について、個人を正確に確認する必要がない場合で、単に毎回のアクセスが、同一の者により行われていることを確認しており、「当人認証」における信用度はある程度ある。
該当しない	該当しない	レベルD	・身元確認を行わずにオンラインでアカウントを作成し、アカウントを作成後もアカウントを入力するだけ。（当人認証を行わない。）	本人に関する情報は不要

4-2. 手法例（法人等に係る行政手続） ～ Step4

①必要な保証レベル		②オンラインによる手法例		③実現できること・特徴
身元確認保証レベル	当人認証保証レベル			
レベル3 対面での身元確認	レベル3 耐タンパ性が確保されたハードウェアトークン	レベルA	・法人代表者等を対面によって確認の上、アカウントを作成し、アカウント作成後は耐タンパ性ハードウェアトークンによる当人確認を実施。 ※耐タンパ性ハードウェアトークンの例： － PIN+ICカード ・申請データに対して、対面によって法人等代表者へ発行された電子証明書(ICカード)を用いて、電子署名を付与。	・行政手続の対象者や行政手続を実施している者について、法人等の基本3情報を毎回確認している。 ・電子署名を検証することにより、非常に高い信用度で「身元確認」を行っている。また、耐タンパ性を有するハードウェアトークンにより、非常に高い信用度で「当人認証」を行っている。
レベル2 遠隔又は対面での身元確認	レベル2 複数の認証要素	レベルB	・法人共通認証基盤における多要素認証の機能を利用する場合等、法人等については、国税庁法人番号公表サイトで商号、所在地及び法人番号を確認し、法人等代表者の押印及び印鑑証明書等の郵送による身元確認で、アカウントを作成し、アカウントを作成後は多要素認証による当人認証の実施。 ※多要素認証の例： － ID・パスワード+二経路認証アプリ － ID・パスワード+ワンタイムパスワード生成アプリ － ID・パスワード+生体認証 ・申請データに対して、法人等代表者へ発行された電子証明書を用いて、電子署名を付与。	・行政手続の対象者や行政手続を実施している者について、登録時に法人等の基本3情報を確認し、認証プロセス時には、登録時の法人等と同一であることを確認している。 ・特に法人共通認証基盤においては、登録時に法人等を相当程度の信用度で「身元確認」を行い、多要素認証の機能を用いることで、相当程度の信用度で「当人認証」を行っている。
レベル1 身元確認のない自己表明	レベル1 単一又は複数の認証要素	レベルC	・法人共通認証基盤における単要素認証の機能を利用する場合等、身元確認を行わずにオンラインでアカウントを作成し、アカウント作成後は単要素認証で当人認証を実施。 ※単要素認証の例： － ID・パスワードのみ － 認証デバイスのみ － 生体認証のみ	・行政手続の対象者や行政手続を実施している者について、法人等を正確に確認する必要がない場合で、単に毎回のアクセスが、同一の者により行われていることを確認しており、「当人認証」における信用度はある程度ある。