電子署名WG 13:10-13:45〈35分〉

電子契約サービスは
弁護士がいないと安心できないのか？

～真正性を保証する技術と運用の解説書～

2020年1月21日

JNSA 電子署名WG
日本トラストテクノロジー協議会（JT2A）
小川 博久

本日のまとめ

1 論点

何を話すのか？
→弁護士がいないと電子契約サービスは安心じゃない？

2 主張

何が言いたいのか？
→弁護士がいても証拠が必要

3 根拠

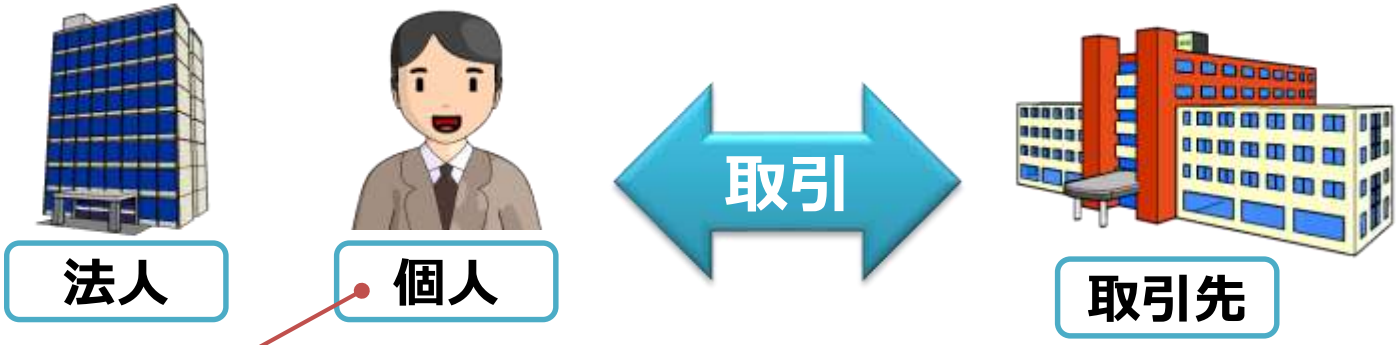
何で言えるのか？
→証拠の確保に使える「真正性を保証する技術」がある

4 今後

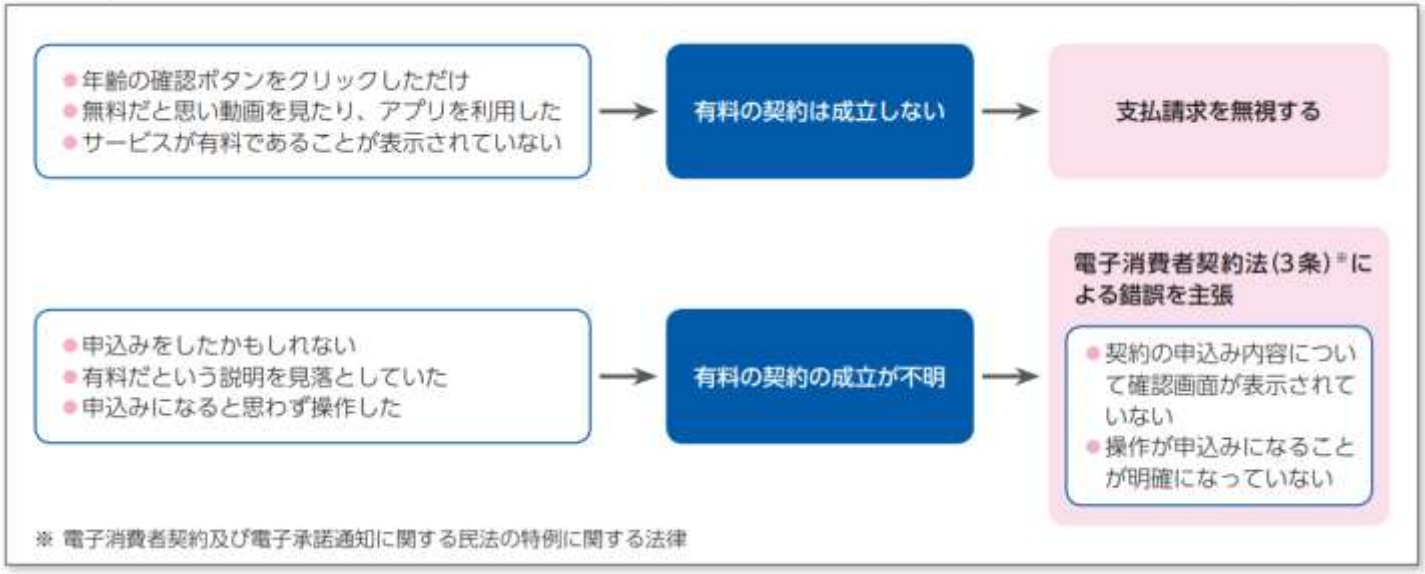
どうするのか？
→真正性を理解＝真正性保証ガイドラインをみてほしい

1.電子契約・取引

契約や取引には様々なトラブルが考えられるが、契約の成立は重要問題
そこで、弁護士がいたほうが安心できる



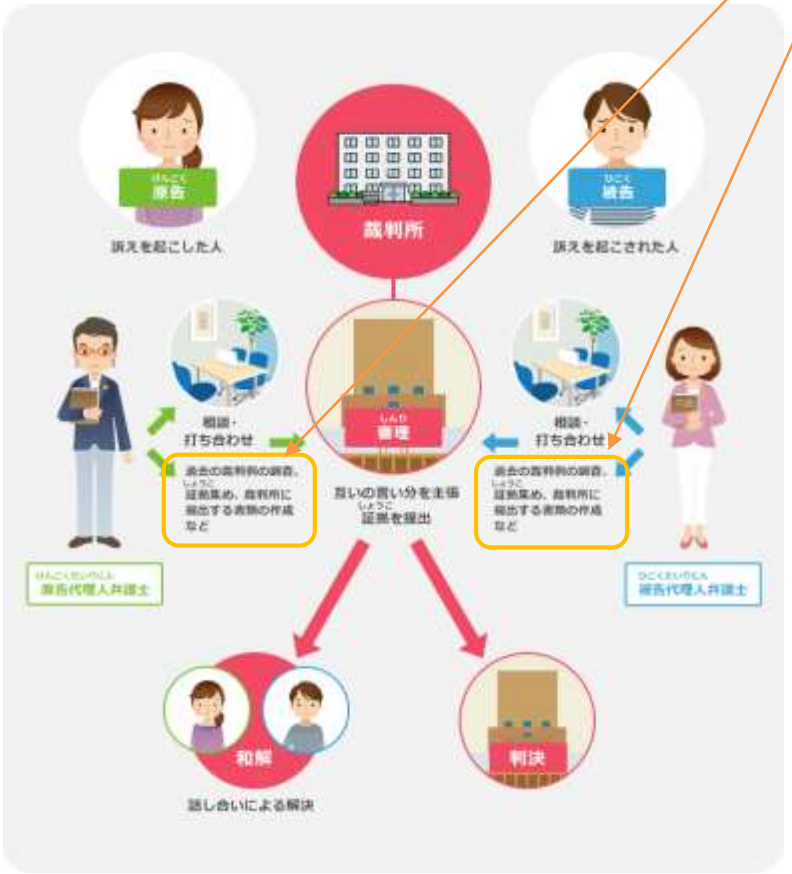
ネット上の契約成立の有無と支払請求への対応



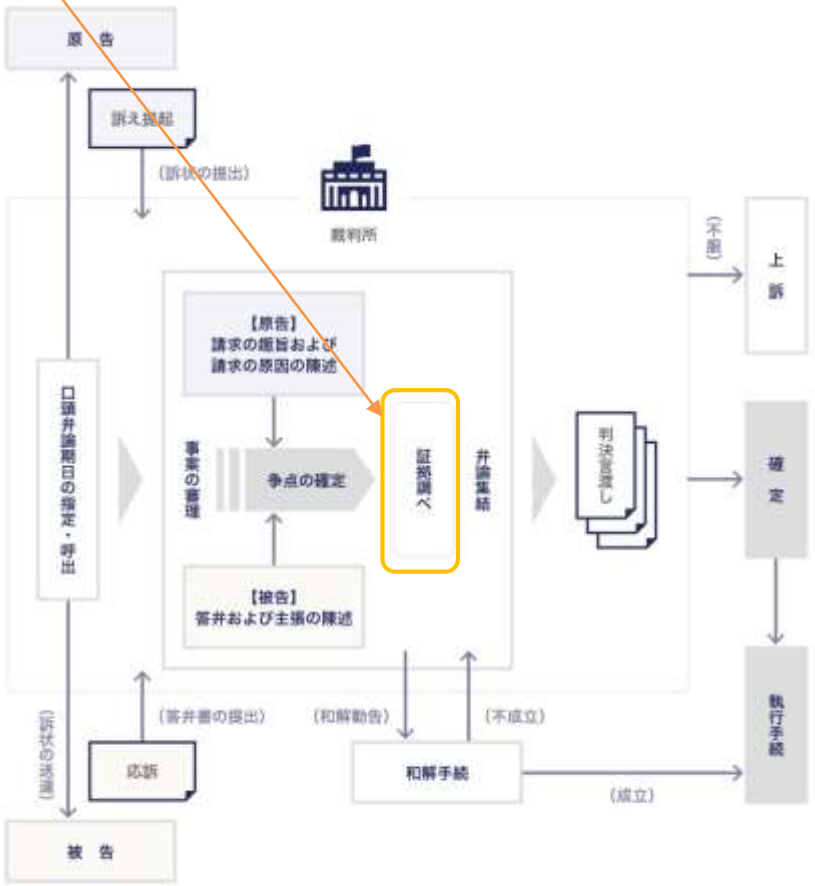
引用：架空請求に関する契約の成立と支払請求の問題
http://www.kokusen.go.jp/wko/pdf/wko-201604_02.pdf

2.弁護士への相談にも証拠が必要

弁護士がまずやることは証拠集め



引用：日本弁護士連合会：裁判ってなぁに？
https://www.nichibenren.or.jp/ja/kids/saiban.html



引用：訴訟の開始から終了までの大まかな流れと期間 - BUSINESS LAWYERS
https://www.businesslawyers.jp/practices/775

証拠とはなにか？　（本人認証の例）

法人

個人

取引先

2

利用される**真正性保証に関する技術**の記載

- 預貯金口座の開設
- 大口現金取引
- クレジットカード交付契約の締結

などの取引の場合、
犯罪による収益の移転防止に関する法律
の対象となり、**本人特定事項の確認**が求められる。

1

関係する**法規則／ガイドライン**の記載

- **商業登記法**に基づく電子証明書による**電子署名**の確認
- ・・・

法人

電子署名法／公的個人認証法に基づく電子証明書による**電子署名**の確認

- ・・・

個人

証拠とはなにか？　（電子署名の例）

JT2A

3

署名生成

生成／検証等の**処理の流れ**の記載

署名検証

4

開発／利用する際の
留意点の記載

危殆化していない
アルゴリズムを
開発／利用すること

秘密鍵

証明書

公開鍵

データ

署名
生成

印

署名

署名
データ

署名
検証

成功

失敗

検証結果

以下の特長を持つ
- 完全性
- 否認防止

5

完全性等の**真正性技術の性質**の記載

標準フォーマットを
開発／利用すること

署名
データ
生成

印

署名
データ

真正性の定義とは？

- 「**ISO27000**」では、
  - エンティティは、**それが主張する通りのもの**であるという特性。
- 「**Wikipediaの情報セキュリティ**」の項目では、
  - ある主体又は資源が、**主張どおりであることを確実**にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
  - 情報システムの利用者が、**確実に本人であることを確認**し、**なりすましを防止**すること
- 「**医療情報システムの安全管理に関するガイドライン**」では、
  - 真正性とは、**正当な権限**において作成された記録に対し、**虚偽入力**、**書換え**、**消去**及び**混同が防止**されており、かつ、第三者から見て**作成の責任の所在が明確**であることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。

結構バラバラ…

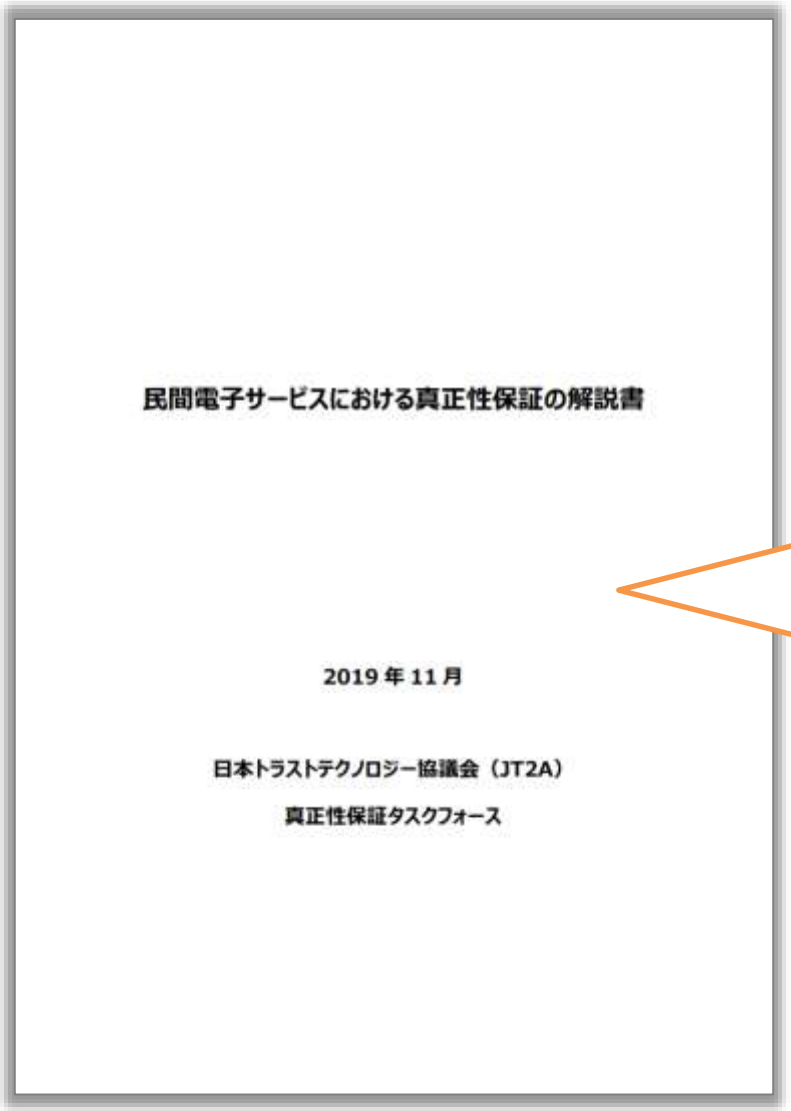
真正性の定義とは？

6

真正性の定義の記載

- 「**ISO27000**」では、
  - エンティティは、**それが主張する通りのもの**であるという特性。
- 「**Wikipediaの情報セキュリティ**」の項目では、
  - ある主体又は資源が、**主張どおりであることを確実**にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
  - 情報システムの利用者が、**確実に本人であることを確認**し、**なりすましを防止**すること
- 「**医療情報システムの安全管理に関するガイドライン**」では、
  - 真正性とは、**正当な権限**において作成された記録に対し、**虚偽入力**、**書換え**、**消去**及び**混同が防止**されており、かつ、第三者から見て**作成の責任の所在が明確**であることである。なお、混同とは、患者を取り違えた記録がなされたり記録された情報間での関連性を誤ったりすることをいう。

3.民間電子サービスにおける真正性保証の解説書



1. 真正性の定義
2. ユースケースと
   関連法規則／ガイドライン
3. 真正性保証に関する技術
4. 真正性技術の性質
5. 処理の流れ
6. 開発／利用する際の留意点

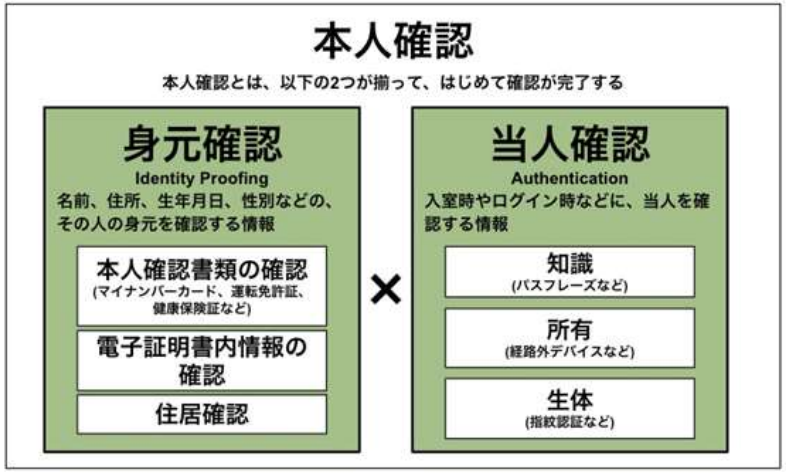
民間電子サービスにおける真正性保証の解説書
https://www.jnsa.org/result/jt2a/

3章 真正性の保証が求められるケースの例

3.1 電子申請（例：e-Gov）
3.2 電子入札（例：GEPS）
3.3 電子処方箋
3.4 本人確認

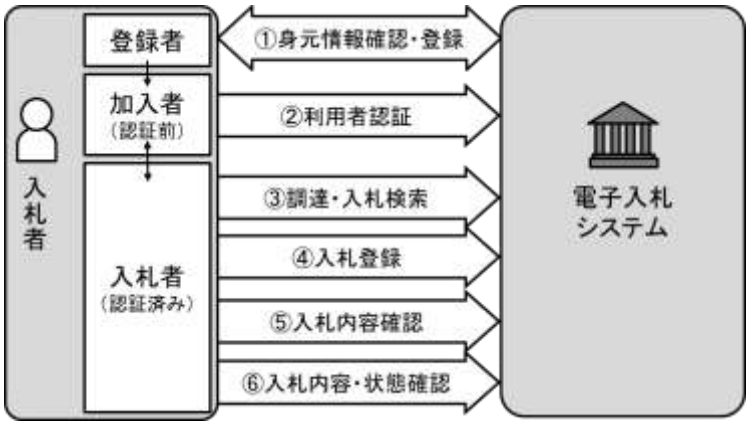
電子政府の総合窓口 「e-Gov」
http://www.e-gov.go.jp/

政府電子調達「GEPS」
https://www.geps.go.jp/introduction

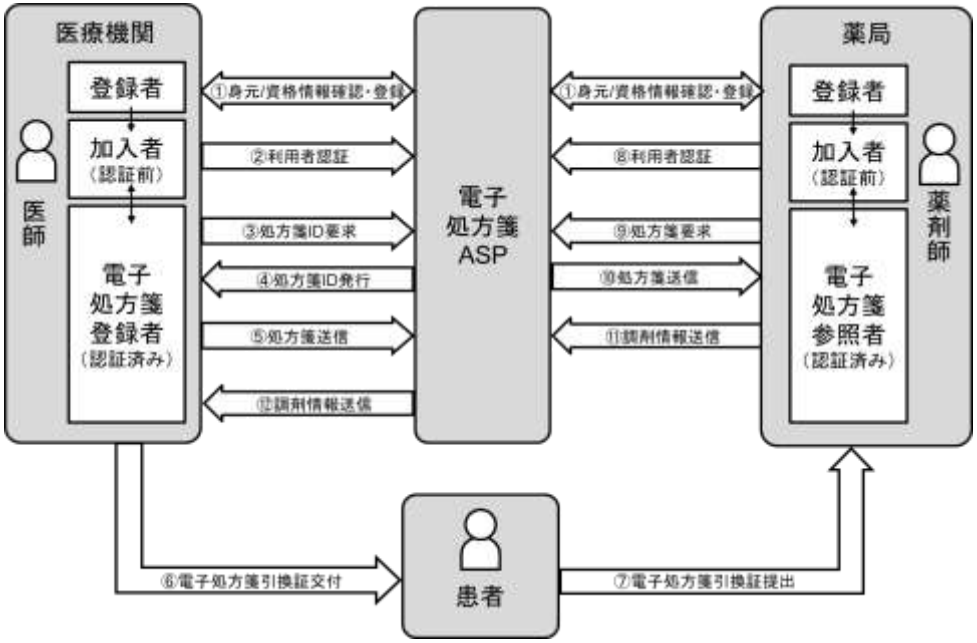


本人確認の分類

3章 真正性の保証が求められるケースの例



電子入札システムの処理例



電子処方箋の処理

4章 真正性保証のレベルの定義

- 保証レベルの選択は想定リスクごとに影響度を判定し、身元確認保証レベル（IAL）、当人認証保証レベル（AAL）を選択する。NIST SP 800-63-3の選択プロセスを記載。

図 A-10 NIST SP800-63-3 の IAL の選択概要図

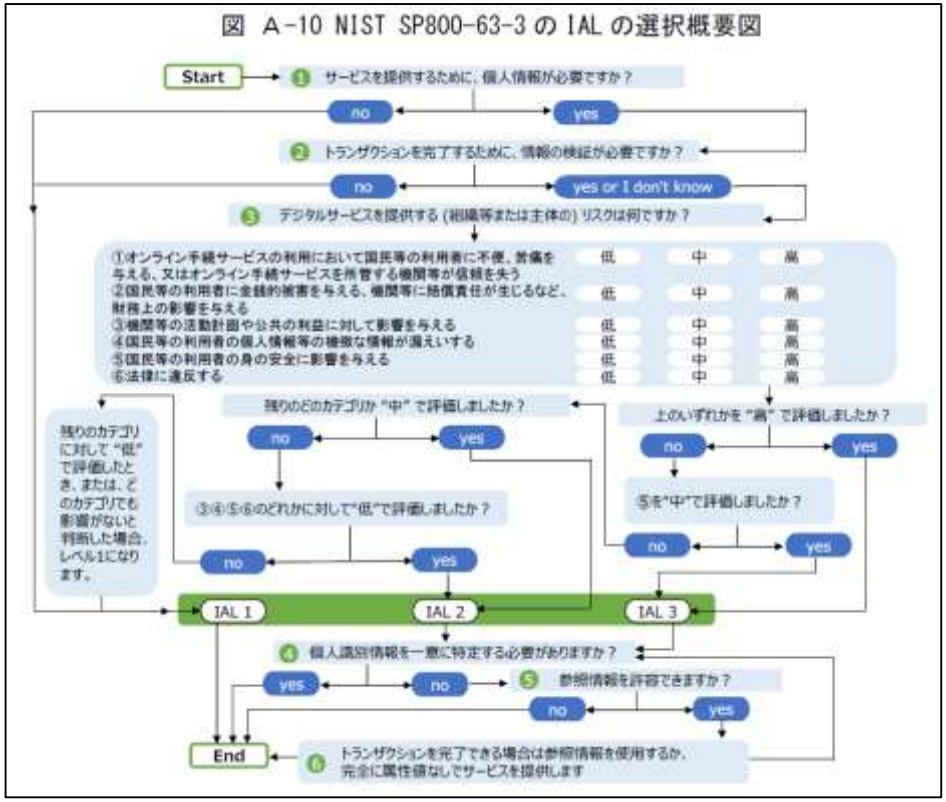
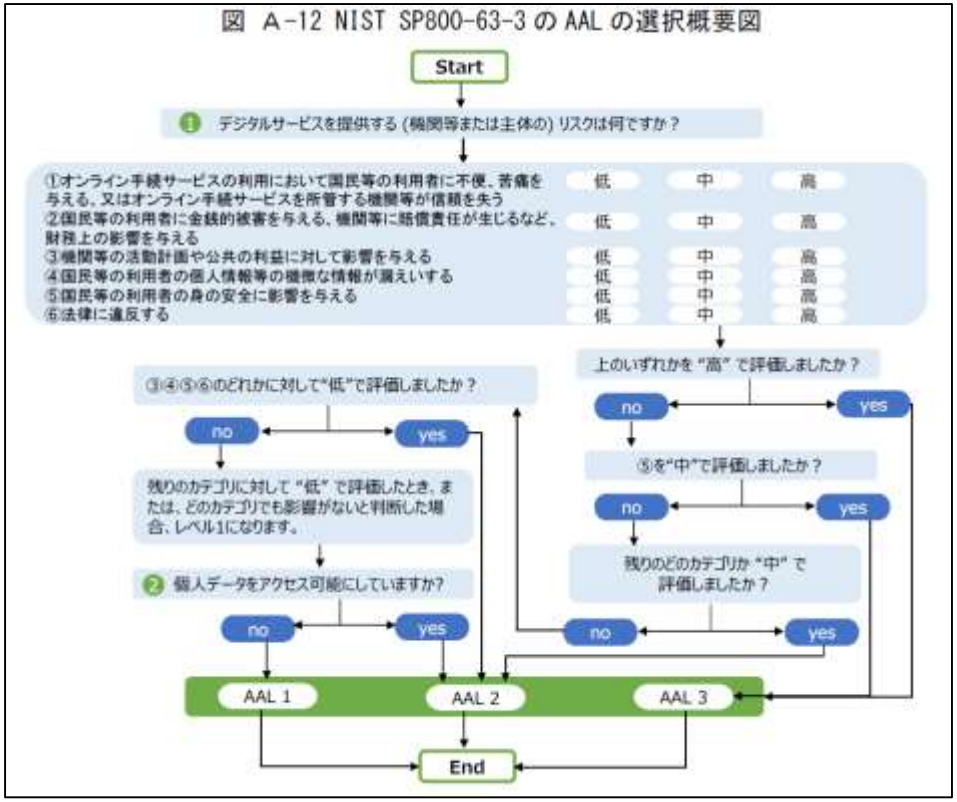


図 A-12 NIST SP800-63-3 の AAL の選択概要図

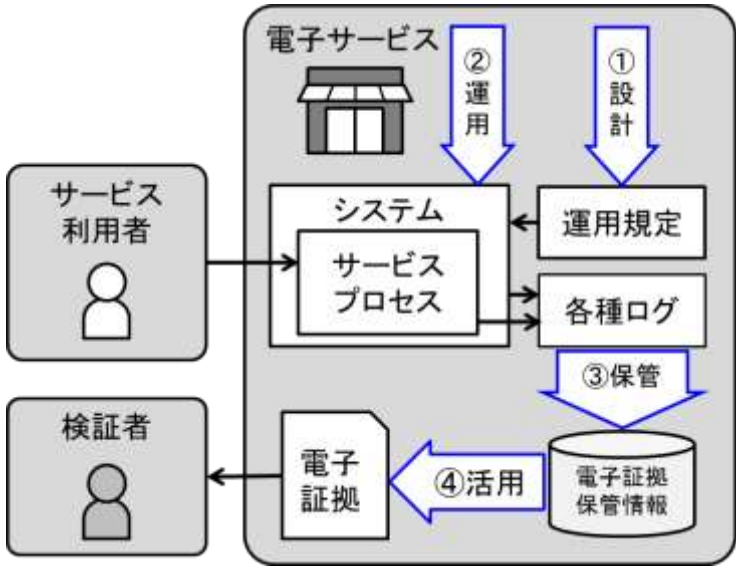


5章 真正性を保証するための実装方法

5.1 電子署名
5.2 タイムスタンプ
5.3 電子認証
5.4 電子証拠
5.5 電子サイン
5.6 組織（属性）確認
5.7 閾値暗号

電子証拠

一般に証拠とは「（裁判において裁判官が）事実の認定を行う為に判断を下す根拠となる資料」とされている。電子サービスにおいて資料は電子情報となり「電子証拠（Electronic Evidence）」または「デジタル証拠（Digital Evidence）」と呼ばれる。適正な電子証拠を保全することにより完全性や否認防止を実現することが可能となる。

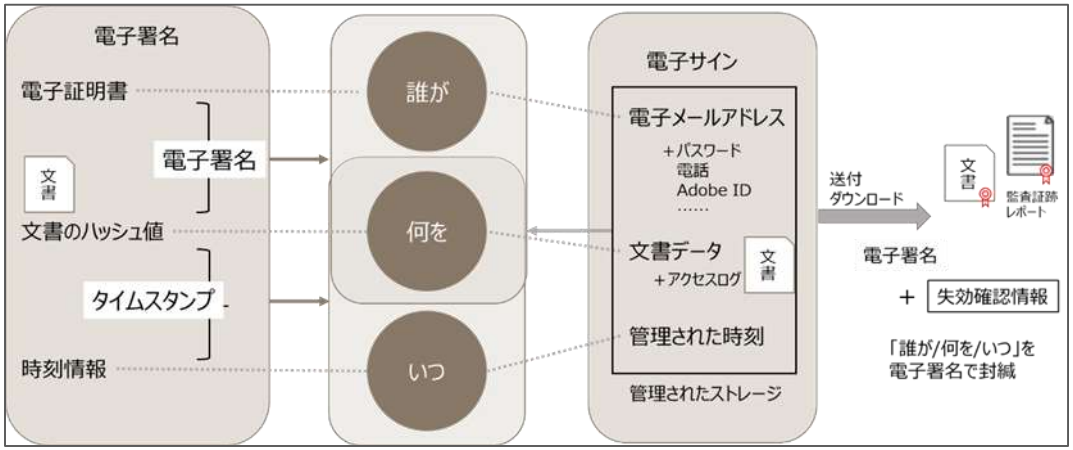


電子証拠の利用フロー

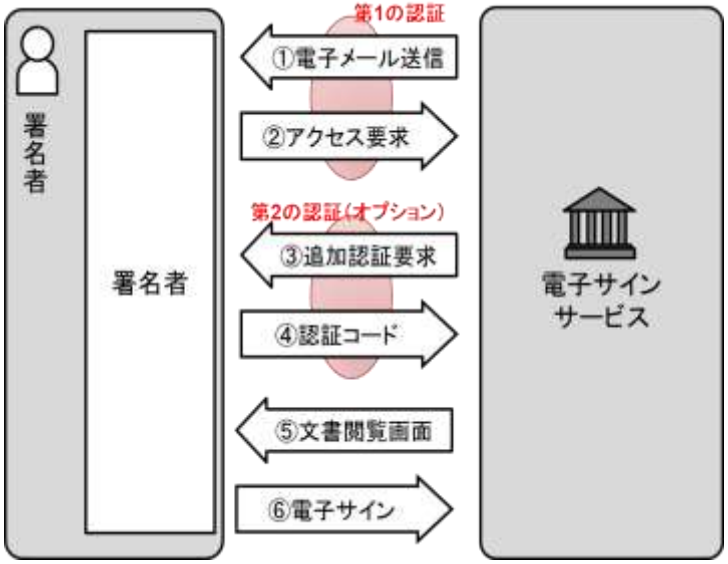
5章 真正性を保証するための実装方法

電子サイン

サイ電子サインには、ペンタブレットを使用した手書きの筆跡を生体情報として記録するものがあるが、ここでは、手書きサインや印影イメージを署名の意思を示す入力情報として使用するものの、サービス利用者を識別するID情報により本人性を確認し、署名対象の文書と紐づけて保管するサービスを電子サインとして説明する。



電子サインの特長（電子署名との対比）



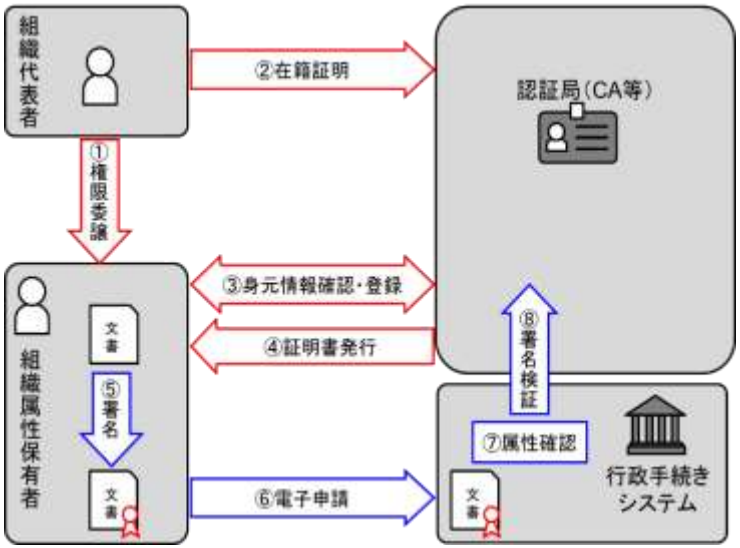
電子サインの認証処理

電子サインの開発時、利用時の留意点

【1】サービス加入者の登録と認証
【2】署名者の身元情報と認証
【3】電子サインを利用することによる完全性と真正性の確保
【4】保管すべきデジタル記録

属性（組織）の確認

組織（属性）とは、個人が所属する組織や役職などを指し、従業員が組織としての意思表示（契約など）を行う場合に利用される。電子証明書の属性情報や電子委任状内の情報、属性管理サーバから発行される情報（アサーション等）により、確認することができる。いずれの技術もデジタル署名やサーバ認証などが施され、組織（属性）情報の完全性の保証を担保している。本節では電子証明書に組織（属性）情報を格納する例を挙げて説明する。



属性（組織）の確認モデル（電子証明書方式）

名称	説明
組織名	「商業登記簿」の「商号」や個人事業主の「屋号」
組織住所	「商業登記簿」の「本店」の住所
組織番号	企業を一意に識別可能な番号 例：法人番号（国税庁が付番） 会社法人等番号（法務局が付番） LEI（Legal Entity Identifier：取引主体識別コード） 株式会社帝国データバンクの TDB 企業コード 一般財団法人日本情報経済 社会推進協会の標準企業コード
部門名	部局や部課など
部門住所	上記「組織住所」以外の部門住所
メールアドレス	申請を受けたメールアドレス
代表者名	組織の代表者氏名
代表者肩書	組織代表者の肩書
役職肩書	役職（組織代表者以外の場合）

主な組織属性

※出典：電子証明書に格納された属性情報の信頼性と利用に関するガイドライン（電子認証局会議 属性ガイドライン検討会）

本日のまとめ

1 論点

何を話したかったのか？
→弁護士がいないと電子契約サービスは安心じゃない？

2 主張

何が言いたいのか？
→証拠がないと弁護士がいても立証できない
★最低限必要な何か（システム要件など）がある

3 根拠

何で言えるのか？
→真正性を保証する技術がある

4 今後

どうするのか？
→真正性を理解＝真正性保証ガイドラインをみてほしい

JT2Aの概要

名称	日本トラストテクノロジー協議会 Japan Trust Technology Association（略称：JT2A） http://www.jt2a.org/
事務局	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（略称：JNSA） 〒105-0003　東京都港区西新橋1-22-12　JCビル4F　E-Mail：sec@jnsa.org
設立	2018年06月　（準備会：2017年11月）
代表者	手塚 悟（慶應義塾大学 環境情報学部 教授）
副代表	松本 泰（セコム株式会社 IS研究所/JNSA PKI相互運用技術WGリーダー）
運営委員長	小川 博久（JNSA電子署名WGサブリーダー） E-Mail：ogawa@jt2a.org
目的	電子署名や電子証明書など含むトラストテクノロジーに関連する事業者及び利用者が主体となり、産学官及び国内外の関連団体と連携して信頼性を担保するための技術等の検討を行い、より信頼できる電子社会の促進に寄与する。
事業内容	・トラストテクノロジー関連ガイドラインの検討及び策定 ・国内外の関連団体と連携し普及、及び利用促進 ・トラストテクノロジーの普及促進のために意見交換や情報共有 ・トラストテクノロジーに関する調査検討、研究開発

参考資料
政府のガイドライン

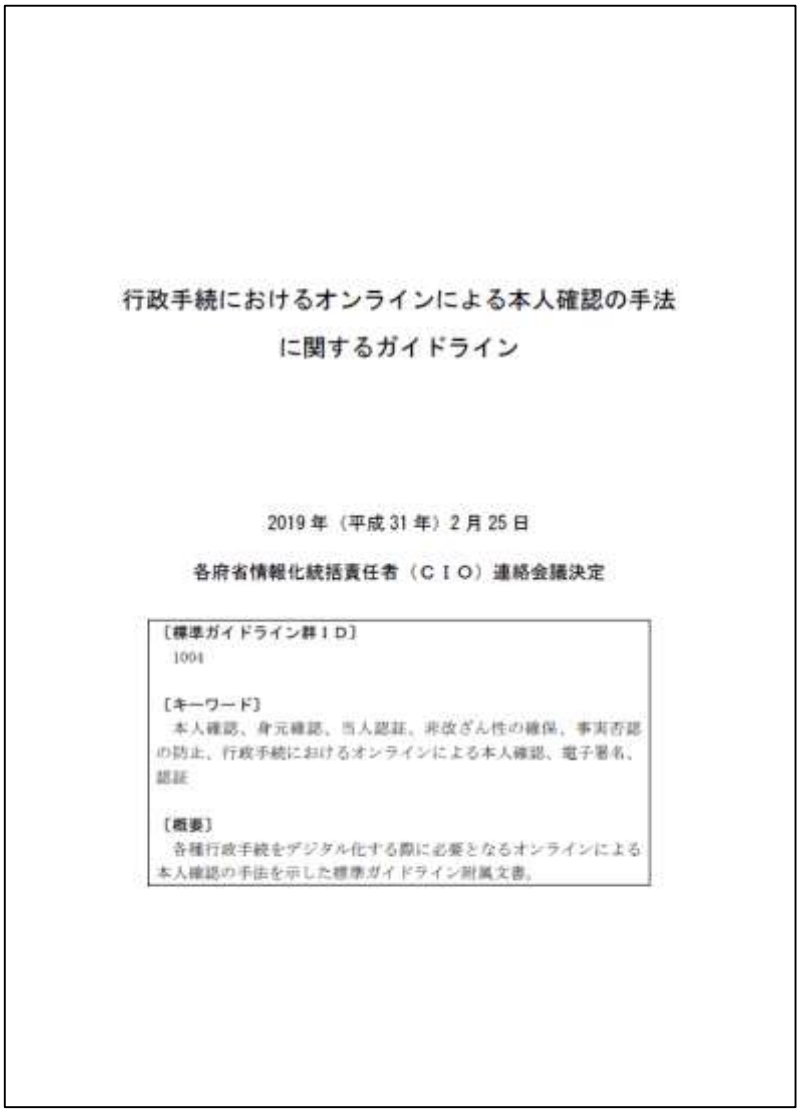
行政手続におけるオンラインによる本人確認の手法に関するガイドライン

「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」
（平成31年2月25日：各府省情報化統括責任者（CIO）連絡会議決定）

各種行政手続きをデジタル化する際に必要となるオンラインによる本人確認の手法を示した文書。

本ガイドラインは決定日から施行される。
以下を規定。

1. 「リスクの影響度」を導出する手法
2. 認証方式の「保証レベル」を導出する手法
3. 認証方式の各保証レベルにて求められる「対策基準」



行政手続におけるオンラインによる本人確認の手法
に関するガイドライン

2019 年（平成 31 年）2 月 25 日

各府省情報化統括責任者（ＣＩＯ）連絡会議決定

［標準ガイドライン群ＩＤ］
1004

［キーワード］
本人確認、身元確認、当人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証

［概要］
各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドライン附属文書。

引用：行政手続におけるオンラインによる本人確認の手法に関するガイドライン
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf

保証レベルに応じた対策基準

付録C　保証レベルに応じた対策基準の概要

- 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

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（※３）
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合 ・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 ※本人限定受取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（又は他２種）の提示 ・申請情報の台帳（又は公的証明書）照合 （郵送又はオンラインの場合） ・申請書に対する電子署名（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、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全て満たす必要がある。
※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に対応する認証方式の選択も可能と考えられる。

引用：行政手続におけるオンラインによる本人確認の手法に関するガイドライン
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf

オンラインにおける本人確認の手法例（個人）JT2A

別紙２　オンラインにおける本人確認の手法例の対応表（個人に係る行政手続）

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：署名用電子証明書)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イ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、アカウントを作成し、アカウント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

オンラインにおける本人確認の手法例（法人）JT2A

別紙３　オンラインにおける本人確認の手法例の対応表（法人等に係る行政手続）

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	・法人等代表者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の法人等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。