資料３－１

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

# （議題３）医療情報システムの安全管理に関するガイドラインの改定に向けた取組状況について

厚生労働省

Ministry of Health, Labour and Welfare of Japan

# 第２回医療・介護・感染症対策WGでいただいたご指摘

○　電子署名の要件として、電子署名法第３条を引用し、実印相当なものを求める必要があるのか。現行の運用において印鑑が実印を要求している場合に、電子署名法第３条の要件を求めることはあっても、現行の運用で実印を求めていないケースについて、特段理由なく実印相当の要件に変えていくということは、他の分野ではほとんど行われていない。

○　電子署名法第３条は、適用された場合に推定されるというものであって、「電子署名」の要件として課すものではない。

○　「医師等の国家資格の確認が電子的に検証できる電子署名」について、電子署名サービス提供事業者には医師登録原簿等との都度照会を求めるものではないということでよいか。

○　事業者による利用者の実在性等の確認については、電子署名法施行規則第５条１項又は第２項の「利用者の真偽の確認の方法」による旨が記載されているが、同条は認定認証事業者に係る基準であるところ、必ずしもこれだけが電子署名として適当というわけではなく、立会人型であっても電子署名法第２条・第３条の要件を満たすものはあるのではないか。

○　立会人型について電子署名法施行規則第５条を求めた場合、立会人型電子署名サービス提供事業者を排除することにならないか

○　外部評価について、具体的な対象項目、評価の程度等が示されていない

○　電子カルテシステムへのログインの際に医師の本人確認・資格確認が行われることをもって、電子署名を不要とすることについても、早急に検討を行う必要があるのではないか。

○　「最低限のガイドライン」の記載ぶりでは外部NWと接続できるものは閉域網の場合だけであるように思える。オープンNWを使う場合における要件を別途立てることが必要ではないか。また、VPN接続を前提としているかのような記載にも思われる。

# 第２回WGの御指摘への検討の方向性【電子署名関係】①

## 電子署名法第３条について

○　医療分野における電子署名に係る争訟が生じた場合、法第３条が適用される場合、立証責任の軽減につながりうるため、改定案においては法第３条を「A 制度上の要求事項」として記載することを検討していたところ。

○　法第３条は法第２条第１項の「電子署名」に固有性の要件などが付加された場合に、真正に成立したものと推定されることを規定したもの。

○　上記と、第３条の適用の前提（※）について、医療機関が理解しておくことは重要ではないか。

（※）　十分な暗号強度を有し他人が容易に同一の鍵を作成できないものであることや、電子署名が本人の意思に基づき行われたものであること等の措置

○　「B　考え方」として記載することを検討する。

● 電子署名及び認証業務に関する法律（平成12年法律第102号）（抄）

第二章　電磁的記録の真正な成立の推定

第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

## 事業者による資格確認時期について

○　事業者による利用者の医師等の国家資格保有の確認は登録時に行うことを想定しており、その旨を明示的に記載することについて改めて検討する。

# 第２回WGの御指摘への検討の方向性【電子署名関係】 ②

## 電子署名法施行規則第５条について

○　医療分野については、国民の身体・生命に影響が生じることなどから、身元確認の信用度が相当程度以上あることが求められるため、改定案においては電子署名法施行規則第５条によることを検討していたところ。

○　前回いただいた、施行規則第５条そのものを要件とすることは過重な負担である旨のご指摘を踏まえるとともに、医療分野におけるオンライン手続に関わるリスクを低減する観点から、 NIST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を踏まえ、以下の水準での確認が求められるのではないか。

・オンライン　：　マイナンバーカード、又は
　　身分証明書（※１）と住民票等の公的証明書をスキャンしたデータ（※２）

・郵送　：　身分証明書のコピー（実印＋印鑑登録証明書）＋　住民票等の公的証明書

・対面　：　身分証明書＋住民票等の公的証明書

（※１）　身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか1種類により、又はその他の身分証明書であれば2種類以上により行うこと

（※２）　いずれも本水準と同等の電子署名を施すこと

○　他方で、施行規則第５条を明記することの必要性については、立会人型電子署名サービス提供事業者における対応が可能であることも確認しつつ、改めて検討する。

## 外部評価について

○　医療情報システムの安全管理に関するガイドラインは考え方を示しているものであり、具体的な評価に関する内容については、本ガイドラインとは別の形で追ってお示しする。

# 第２回WGの御指摘への検討の方向性【電子署名関係】 ③

## 電子カルテシステムへのログインをもって電子署名を不要とすることについて

○　民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（e-文書法）において、法令の規定により署名等をしなければならないとされている書面を電子的記録によって作成する際には、主務省令で定めるものをもって当該署名等に代えることができるとされている。

○　厚生労働省の定める主務省令（厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令）においては、これ（注：主務省令で定めるもの）を電子署名としている。

※　厚生労働省以外の府省においても同じく電子署名としている。

○　医療に係る文書では、処方箋、死亡診断書等が、法令で記名押印又は署名を求めている文書に該当するため、e-文書法に基づき、これらの文書には電子署名が必要。

○　医療情報システムの安全管理に関するガイドラインは、e-文書法を前提として、利用可能である電子署名を示している。

# 第２回WGの御指摘への検討の方向性【外部NW関係】

○　「最低限のガイドライン」の記載ぶりでは外部NWと接続できるものは閉域網の場合だけであるように思える。オープンNWを使う場合における要件を別途立てることが必要ではないか。また、VPN接続を前提としているかのような記載にも思われる。

○　ご指摘を踏まえ、分かりやすく、また必要以上に慎重にならないような表現等に修正することを検討する。

・「クローズドなネットワーク（閉域網）以外に、オープンなネットワークを選択する場合」、さらに、「オープンなネットワークを選択し、VPN接続を利用しない場合」等、明示的に区別した記載をし、具体的な対策が分かりやすくなるよう記載の修正を検討する。

・外部ネットワークの選択に応じた対策の整理や、例示としての記載の明確化、医療機関等が必要以上に慎重にならないような表現になるよう、記載の修正を検討する。

Ministry of Health, Labour and Welfare of Japan

# 参考資料

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

# 身元確認保証レベル等の選択に係る考え方について

## デジタル・ガバメント実行計画（平成30年7月20日 デジタル・ガバメント閣僚会議決定）

4 プラットフォーム改革

4.2 システム基盤の整備

2) 本人確認等の手法の見直し（◎内閣官房、経済産業省、全府省）

電子的な本人確認等の手段についても、行政手続における本人確認等の手法として広く用いられているマイナンバーカード等を用いた電子署名に加え、情報システムの取り扱う情報や行政サービスの性質等を勘案し、電子署名以外の電子認証等の適切な技術選択を行うことが重要である。また、電子認証に関しては、近年技術標準の検討も進んでおり、国際的な標準化（米国NIST SP800-63-3等）とも整合性を持った取組を推進する必要がある。

上記の背景を踏まえ、内閣官房において、2018年（平成30年）内に本人確認等の手法の見直しに関する方針を整理するとともに、2018年度を目途に、「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」（平成22年8月31日CIO連絡会議決定）の見直しを行う。各府省は、本見直しを踏まえ、保有する手続において本人確認等の手法の見直しを実施し、内閣官房は、法令の改正における雛型の提示など、各府省の見直しへの支援を行う。この際、マイナンバーカードに搭載された公的個人認証や、同カードと電子委任状を活用した代理権を確認できる仕組みなど、新たな本人確認手法を含む様々な選択肢を考慮に入れる。

## 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CIO連絡会議決定）

2 オンラインによる本人確認の手法を決定するための進め方（個人の場合）（※）

2.2 オンラインによる本人確認に必要な保証レベルの判定

2) 対象となるオンライン手続で想定される脅威についてリスク評価を行う。

具体的なリスク評価は、「付録A．認証方式の合理的な選択を目的としたリスク評価手法」の「7 各リスクの種類による影響度の導出」までの内容に基づいて行う。

3) 対象となるオンライン手続の認証強度として求められるレベル（保証レベル）を判定する。

保証レベルは上記2)の結果を用いて「身元確認保証レベル」と「当人認証保証レベル」とをそれぞれ判定する。具体的な判定は、「付録A．認証方式の合理的な選択を目的としたリスク評価方法」の「8 身元確認保証レベル（IAL（Identity Assurance Level））の選択」以降に基づいて行う。

（※） 法人の場合も同様

# 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における保証レベル判定・リスク評価

## 保証レベル判定（身元確認保証）

図 A-10 NIST SP800-63-3 の IAL の選択概要図

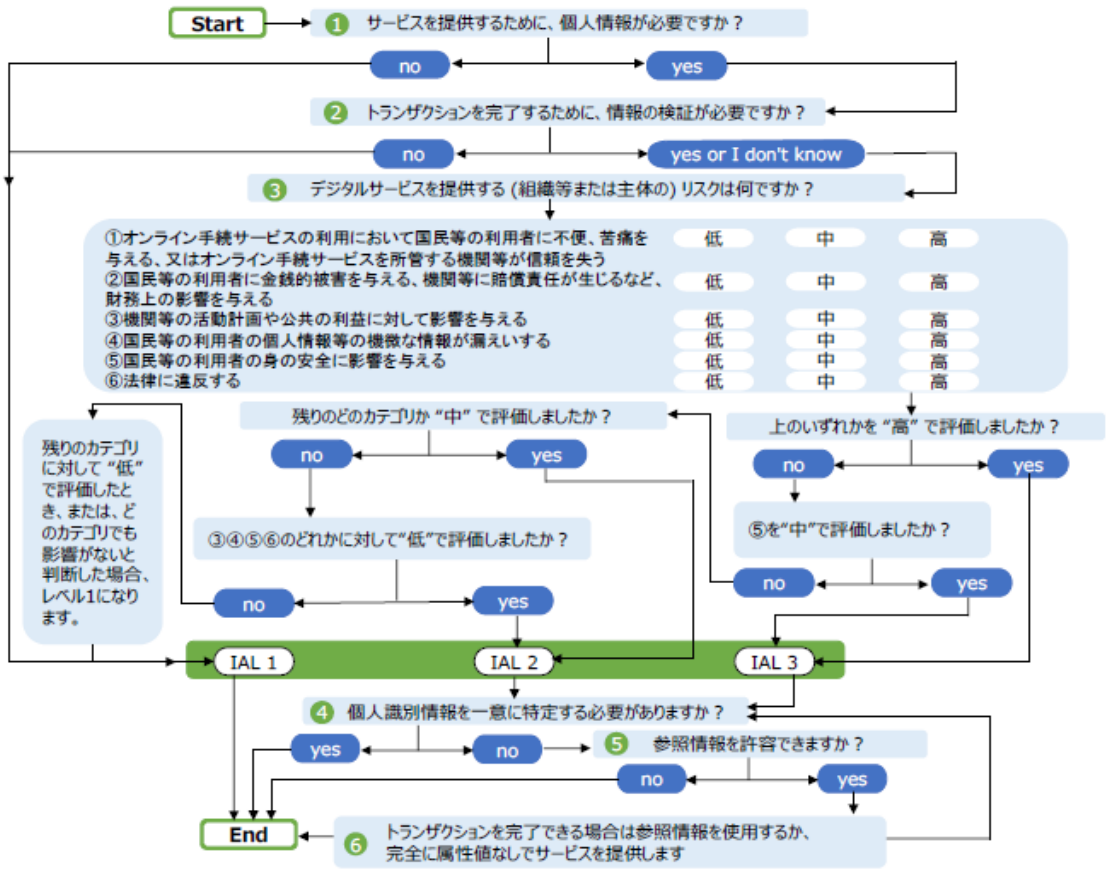


表 A-11 身元確認保証レベル（IAL）の概要

| 身元確認保証レベル | レベルの定義 |
|---|---|
| レベル 1<br>（IAL1） | 身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。 |
| レベル 2<br>（IAL 2） | 身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。 |
| レベル 3<br>（IAL 3） | 身元識別情報が、特定された担当者の対面で確認され、身元確認の信用度が非常に高い。 |

出典）「デジタルアイデンティティガイドライン（NIST SP800-63-3）」より作成

（※） 当人認証保証レベルでも概ね同様の判定が行われる

表 2-3 保証レベルと手法例の対応付け[2]（個人）

| 必要な保証レベル | | オンラインによる手法例 |
|---|---|---|
| 身元確認保証レベル | 当人認証保証レベル | |
| レベル 3<br>対面での身元確認 | レベル 3<br>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 |
| レベル 2<br>遠隔又は対面での身元確認 | レベル 2<br>複数の認証要素 | レベル B |
| レベル 1<br>身元確認のない自己表明 | レベル 1<br>単一又は複数の認証要素 | レベル C |
| 該当しない | 該当しない | レベル D |

○ 医療分野におけるオンライン手続に関わるリスクを低減する観点から、情報セキュリティ分野で国際的に信頼性の高いNISTガイドラインを踏まえた対応が必要。

○ 医療分野においては、少なくともレベルB以上のオンラインによる手法が求められる。