資料２－１

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

第13回 健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

２０２２（令和４）年１２月１５日

「医療情報システムの安全管理に関するガイドライン」について

医政局 特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

・ガイドライン 改定

第12回 健康・医療・介護情報利活用検討会
医療等情報利活用WG
（令和４年９月５日）資料１（一部改変）

第5.2版 から 第6.0版 への改定方針

2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、本ガイドラインに記載されているネットワーク関連のセキュリティ対策が必要となる。これを踏まえ、第6.0版への改定では、第5.2版で中長期的に検討を継続することとした論点を中心に、全体構成の見直しとともに検討する。

○ 外部委託、外部サービスの利用に関する整理

- クラウドサービスの特徴を踏まえたリスクや対策の考え方
- 医療機関等のシステム類型別に対応した責任等の整理　　等

○ 情報セキュリティに関する考え方の整理

- ネットワーク境界防御型思考／ゼロトラストネットワーク型思考
- 災害、サイバー攻撃、システム障害等の非常時に対する対応や対策
- 本人確認を要する場面での運用（eKYCの活用）　　等

○ 新技術、制度・規格の変更への対応

- オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置
- 新たなネットワーク技術（ローカル５G）の利用可能性、利用場面
- 医療情報の共有・提供に関連する法令等の規定や技術・規格の動向

○ 全体構成の見直し

- 経営管理（Governance）編、企画管理（Management）編、システム運用（Control）編の３編構成
- Q&Aの整備、読者類型ごとの参照先等を示した読み方支援文書等の作成

※ 各編は数十ページ程度を想定（第5.2版の文章等を全面的に精査）
第5.2版 6.12章（電子署名）は、策定時に詳細な検討・調整を行ったため、原則、現行版を踏襲

外部委託、外部サービスの利用に関する整理　（１／２）

論点	背景 → 対応方針	対応内容
クラウドサービスの特徴を踏まえたリスクや対策の考え方	・第5.2版では、必ずしもクラウドサービスにおける対策等を個別に分けて記載していない。 ↓ ・クラウド技術を利用したサービス固有のリスクや対策について整理する。（例えば仮想技術を利用した資源の利用、共同利用等） ・クラウドサービスにおける対策の特殊性（作業に関する報告等、ソフトウェアのバージョンアップ等）について整理する。	・クラウドサービスの特徴を踏まえた対応などに関して追記等を行った。 企画管理（Management）編 ２．２．２　委託における責任分界（複数事業者が関与する場合を含む） ９．２　機器等の安全性の確認 システム運用（Control）編 ３．２　仕様適合性の確認を踏まえた調整 ３．４　提供される情報システム・サービスに応じた責任分界　等

外部委託、外部サービスの利用に関する整理　（２／２）

論点	背景 → 対応方針	対応内容
医療機関等のシステム類型別に対応した責任等の整理	・第5.2版では、複数ベンダが関与する場合の責任分界についての基本的な考え方が示されているものの、必ずしもオンプレミスとクラウドサービスの利用関係は示されていない。 ・複数ベンダーのシステム・サービスを多重的に利用する際に、医療機関等が行うべきベンダーに対する責任管理が、システムの利用形態の複雑化から難しくなっている。 ↓ ・医療機関等におけるオンプレミスとクラウドサービスの利用形態等について整理する。 ・複数のベンダが関与する場合の責任の取決め等に関する考え方などを整理する。 ・オンプレミスを含めたサービス間連携（API）や、責任分界の考え方等を整理する。 ・医療機関等における複数ベンダーにおける責任管理等の考え方を示す。	・クラウドサービスの特徴を踏まえた対応などに関して追記等を行った。 システム運用（Control）編 ９．１　ソフトウェアの構成管理 １０．１　保守時の対策　　等 ・クラウドサービスに関しては、特に責任共有モデルに関する整理を行い、管理責任の考え方を整理した。 経営管理（Governance）編 ５．３　責任分界管理 企画管理（Management）編 ２．２．２　委託における責任分界（複数事業者が関与する場合を含む） システム運用（Control）編 ３．４　提供される情報システム・サービスに応じた責任分界

情報セキュリティに関する考え方の整理　（１／３）

論点	背景 → 対応方針	対応内容
ネットワーク境界防御型思考／ゼロトラストネットワーク型思考 ※ ゼロトラストとは「何も信頼しない」を前提に対策を講じるセキュリティの考え方。閉域ネットワークであれば安全であるなどの境界防御前提には立たない。	・第5.2版では、内部脅威監視など、ゼロトラストの考え方の一端は示しているものの、境界防御を踏まえた対策等の考え方が中心となっている。 ↓ ・ネットワークの安全性のあり方や認証のあり方を踏まえて、ゼロトラストの考えに則した対策の考え方を示す。 ・内部ネットワークによる利用を中心としている医療機関等と外部サービスの利用を中心としている医療機関等などの違いを踏まえた具体的な対策の考え方を示す。 ・医療情報システムに関わる全ての利用者（保守事業者、患者等を含む。）等を想定した考え方を整理する。	・ネットワーク分類（従来のオープン、クローズ等）についての考え方は、オープンなネットワークと、接続先が限定されているまたは接続先との経路が管理されているネットワークに整理した。 システム運用（Control）編 １３．１　ネットワークに対する安全管理の考え方 ・ネットワーク境界防御型思考に加え、ゼロトラストネットワーク型思考を取り入れ、多層防御思考という方針で整理した。 システム運用（Control）編 １３．１　ネットワークに対する安全管理の考え方 １３．２　不正な通信の検知や遮断、監視

情報セキュリティに関する考え方の整理　（２／３）

論点	背景 → 対応方針	対応内容
災害、サイバー攻撃、システム障害等の非常時に対する対応や対策	・第5.2版では、ランサムウェア対応のほか、マルウェアによる攻撃への対応や、サイバー攻撃時における通報体制等について示されている。 ・医療機関等に対するサイバー攻撃は、さらに巧妙さや対象の拡大が予想される中で、必須の対策があればそれを示す必要がある。 ↓ ・ゼロトラストの議論と併せ、検知の考え方について整理し、実行力がある対応のあり方を整理する。 ・攻撃ルートの多様性を確認し、各ルートにおいて想定されるリスクや対策の考え方を整理する。	・非常時を、災害時、サイバー攻撃時、システム障害時に分けて、運用に関する具体的な対応について整理した。 経営管理（Governance）編 １．３　医療機関等における管理責任 企画管理（Management）編 １１．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定 １２．サイバーセキュリティ システム運用（Control）編 １１．システム運用管理（通常時・非常時等） ・サイバー攻撃に対する対策として、攻撃を検知するため、従来のIDS/IPSのほか、内部脅威監視やファイル無害化処理、EDR等の振る舞い検知などの例示を加えた。 システム運用（Control）編 ９．２　機器等の脆弱性への対策 １８．外部からの攻撃に対する安全管理措置

情報セキュリティに関する考え方の整理　（３／３）

論点	背景 → 対応方針	対応内容
本人確認を要する場面での運用（eKYCの活用）	・オンラインでの本人確認のための技術であるeKYC（electronic Know Your Customer）は、我が国では犯罪収益移転防止法において、利用が認められている。 ・医療情報システムでの利活用においては、様々な場面で利用者の本人確認が求められるが、eKYCの利用について、第5.2版では示されていない。 ↓ ・eKYCの技術的な特徴・役割の特徴等を整理して、eKYCが利用可能と考えられる領域について検討する。 ・医療情報システムの利用（または、そのための手続等）において、eKYCの利用可能性等を検討するほか、これを利用する場合に想定されるリスク等について整理する。	・本人確認の手段の一つとして、eKYCに関する技術的な特徴や役割等を確認し、検討した結果、医療分野において、本人確認が実施される様々な場面を想定し、本人確認の手段に求められる信頼性に関する考え方を示し、Q&AにeKYCなど本人確認の手段を例示する。 企画管理（Management）編 １３．１．２　医療情報システムの利用者の登録と認証

規制改革実施計画（令和４年６月７日 閣議決定）　より抜粋

＜医療・介護・感染症対策＞（２）医療DXの基盤整備（在宅での医療や健康管理の充実）

４．電子処方箋の普及及び医療分野における資格確認・本人確認の円滑化

d）厚生労働省は、医療現場で利用される電子署名について、クラウド型電子署名等を利用しようとする医師が、当該クラウド型電子署名等の利用申込を行う際の本人確認手段として医師が自宅等から手続きを　完結できるようにするため、オンラインで完結可能な本人確認方法であるeKYC（electronic Know Your Customer）を活用できることとする方向で所要の検討を行う。

[令和４年度上期検討・結論]

新技術、制度・規格の変更への対応　（１／２）

論点	背景 → 対応方針	対応内容
オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置	・2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、ネットワーク関連のセキュリティ対策が必要となることから、導入に必要なネットワーク機器等の安全管理措置を示す必要がある。 ↓ ・オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置をまとめ、Q&A等に記載する。	・オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置をQ＆Aに記載するとともに、診療所や小規模医療機関向けの特集を作成する。
新たなネットワーク技術（ローカル５G）の利用可能性、利用場面	・PHSサービスに代わり、5Gサービス が院内ネットワークとして採用される可能性があるため、その対応を図る必要がある。 ↓ ・2019年度ガイドライン改定作業班において新規のセキュリティ課題はないと整理されている一方で、ローカル5Gを導入する場合の無線局免許取得に必要なセキュリティ対応などにおいて、対策を検討すべき旨が指摘されていることを踏まえ、具体的なセキュリティ課題を整理し、検討する。 ・ローカル５G導入に伴う対応と５Gを利用する場合の対応策は異なるところ、ローカル５Gの利用可能性を鑑みて、ガイドライン、Q＆A等での記載要否を判断する。	・ローカル５Gの医療分野での利用について、「５G等の医療分野におけるユースケース　改訂版（案）」（令和３年６月 総務省）などで具体的な利用場面が示されてはいるものの、まだ導入実績等が限られている状況であることが確認された。 ・医療分野でのローカル５Gの利用が進み、具体的な導入実態とともに利用に際した課題等の整理が必要になり次第、Q＆A等に記載する。

新技術、制度・規格の変更への対応　（２／２）

論点	背景 → 対応方針	対応内容
医療情報の共有・提供に関連する法令等の規定や技術・規格の動向	・医療情報連携ネットワークを通じた情報提供について、共同利用型などを想定し、記載を検討する必要が生じる可能性がある。 ↓ ・個人情報保護法等の情報資産管理に関連する法令等の規定や技術・規格の動向を踏まえた考え方や手法の更新があれば、随時検討する。	・令和２年改正個人情報保護法（令和４年４月施行）により手続的要件が変更された内容を確認した。 ・医療情報連携ネットワークにおける共同利用型への対応等の実情を踏まえ、留意点をQ&Aに記載する。

第12回 健康・医療・介護情報利活用検討会
医療等情報利活用WG
（令和４年９月５日）資料１（一部改変）

全体構成の見直し

医療機関等の様々な規模と多様なシステム構成・サービス提供形態を踏まえ、安全な情報資産管理を基礎とし、意思決定・方針策定・戦略立案（Governance）、企画管理・システム運営（Management）、管理方法・運用手段（Control）の３つの視点で整理。

概説 編 Overview

ガイドラインの各編を読むに際して、まずはじめに、前提として必要な知識や各編の基本的な概要をまとめる。

- ガイドラインの目的
- 対象とする情報・文書・システム
- 関連する法令等の規定との関係や経緯
- 各編の位置付けと目次構成、概要 等

経営管理 編 Governance

組織の経営方針を策定し、情報化戦略を立案する経営管理層に必要な考え方や関連法制度等をまとめる。

- 取り扱う情報の重要性と関連法規
- 情報資産管理や情報システム運用に伴い生じる責任・責務
- 情報システムの有用性と安全管理 等

企画管理 編 Management

経営方針・情報化戦略に基づき、システム利用者・管理者・事業者で情報資産を運営、情報化を管理する考え方や方法論をまとめる。

- 情報資産管理体制と責任分界
- リスクアセスメントと対策
- 情報の種類に応じた管理・監査
- 非常時の対応と非常時への対策 等

システム運用 編 Control

安全な情報資産管理やシステム運用を実現するために、関連法制度を遵守した考え方とその実装手法、活用する技術等、具体的な考え方や技術をまとめる。

- 個人情報保護法、e-文書法、電子署名法等により求められる技術
- システム利用者、クライアント側/サーバ側/インフラ領域等それぞれで活用する安全管理対策・措置技術 等

別添 資料 Appendix

- 各編 概要
- 用語集
- Q&A
- ガイドラインの改定と関連法規の遷移
- ガイドラインと関連法規との関係性
- 第5.2版から第6.0版への各項目の移行対応表
- 第6.0版の各編の各項目の相関表
- 診療所・小規模医療機関向けの特集
- 医療機関におけるサイバーセキュリティ・バックアップに関する特集
- サイバーセキュリティ対策チェックリスト
- システム障害発生時の対応フローチャート 等

第6.0版 への改定スケジュール（案）

改定作業班：2022（令和４）年７月１４日、８月１０日、９月１２日、１１月９日 、１２月１日 に開催（計５回）

時期	会議・イベント	主な議事など
12/15(木) （本日）	第13回 健康・医療・介護情報利活用検討会 医療等情報利活用WG	・第6.0版での対応内容、各編（概要）の審議
12月 下旬	第14回 健康・医療・介護情報利活用検討会 医療等情報利活用WG（持ち回り）	・第6.0版パブリックコメント案の審議
1月 上旬～ ２月上旬	第6.0版 パブリックコメント 開始	・パブリックコメント結果を踏まえた 第6.0版 最終案に向けた調整
2月 中旬	第6回 ガイドライン改定作業班	・第6.0版 最終案の確認 ・別添資料に関する検討
2月 中旬～ 2月下旬	第15回 健康・医療・介護情報利活用検討会 医療等情報利活用WG	・第6.0版 最終案、別添資料の審議
2月下旬～ 3月上旬	第6.0版、別添資料 公表	

・保健医療福祉分野での電子署名等

環境整備専門家会議

信頼性に関する基本方針

保健医療福祉分野の特性を念頭に、電子署名等の環境整備に求められる信頼性を以下の通りとする。

信頼性に関する基本方針

保健医療福祉分野における電子署名等の環境整備に求められる信頼性

保健医療福祉分野において取り扱う情報の特性や遵守すべき法令上の規定を踏まえ、
電子署名等に関する、電子証明書の発行時、発行後の利用時等、信頼性が求められる場面において、
NIST Special Publication 800-63 Revision 3「Digital Identity Guidelines」に定義されている

- 身元確認の頑強性（IAL：Identity Assurance Level）：Level 3
- 当人認証の頑強性（AAL：Authentication Assurance Level）：Level 3
- 認証情報連携の確からしさ（FAL：Federation Assurance Level）：Level 3

が求められる。

規定類（規則、様式、基準）

評価方針・基準(案) に基づき、申請事業者側の評価申請規則(案)、専門家会議側の評価実施規則(案)をまとめた。
今後、内閣府 規制改革推進会議の議論等を踏まえ、申請等について検討する予定。

申請事業者 側

評価申請規則に基づく申請

- 評価申請規則：事業者が専門家会議に評価認定を受けるための手順等を記した規則
- 申請書類　　：事業者が申請に際して、表書きとして用いる様式（第１号様式）、
  特定認証業務を行う認定認証事業者である証明書類、事業者（概要）、
  認証局運用規程及び証明書ポリシ（現行版と更新予定版）

専門家会議 側

評価実施規則に基づく評価認定

- 評価実施規則：申請事業者に対して、専門家会議において、評価作業を実施し、
  評価認定を行う手順等を記した規則
- 評価基準　　：申請事業者が提出する書類一式に対し、評価作業を実施する際の基準

  署名方式：ローカル署名、　署名事業：認定認証事業者による電子署名サービス、

  属性証明：認定認証事業者による属性証明書、　属性確認：HPKIサブ認証局と同等の確認手順

（参考）本人確認（身元確認：Identity Assurance Level ＋ 当人認証：Authentication Assurance Level）

両者をあわせて本人確認という

身元確認・当人認証とはなにか

身元確認

ユーザー当人の実在性を確認

- 登録する氏名・住所・生年月日等が正しいことを証明/確認すること

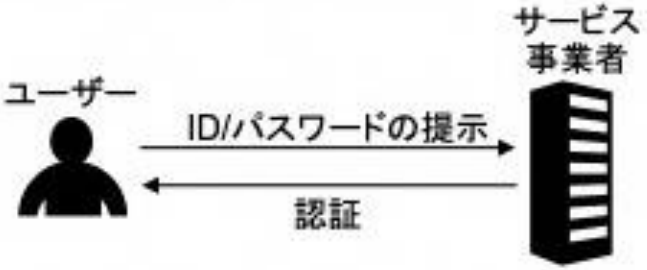
（例）

当人認証

ユーザーの行為を確認

- 認証の3要素[1]のいずれかの照合で、その人が作業していることを示すこと

（例）



（参考）レベル区分[3]

身元確認

保証レベル 高	
Lv3	「対面」で「公的身分証」を基にした身元の確認
Lv2	「郵送等の非対面」で「公的身分証」を活用した身元の確認
Lv1	「自己申告」を基にした身元の確認

当人認証

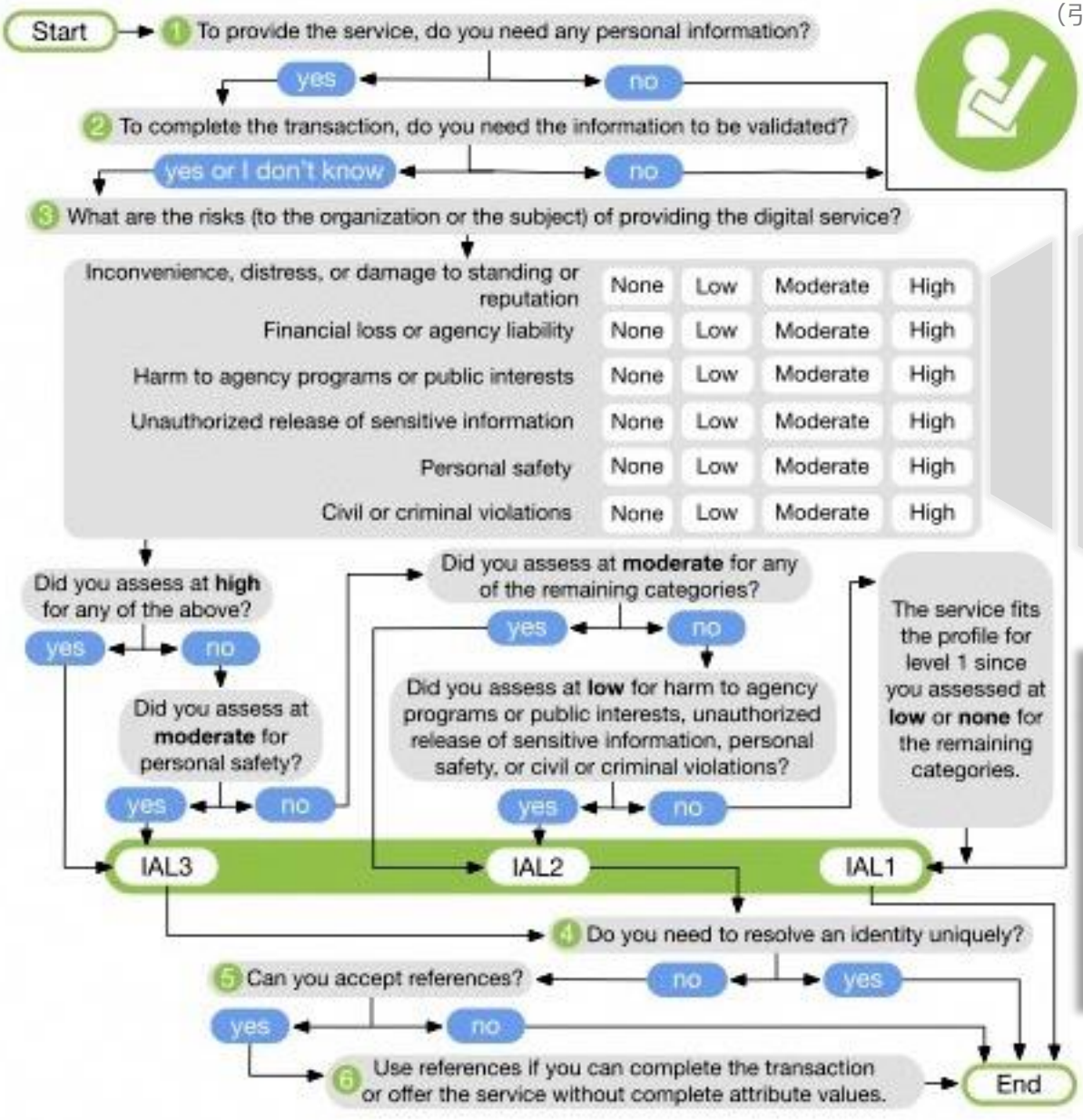
保証レベル 高	
Lv3	3要素のうち耐タンパ性を持つハードウェア[2]を含めた複数を用いる認証
Lv2	3要素のうち複数用いる認証
Lv1	3要素のうち1つ用いる認証

1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「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2月CIO連絡会議決定）のレベル区分

（引用元：経済産業省「オンラインサービスにおける本人確認手法の整理に関する検討報告書」2020/3/31）

（参考）IAL：個人のIdentityを確信を持って決定するための Identity Proofingプロセスの頑強性　の選択

（引用元：NIST: National Institute of Standards and Technology Special Publication 800-63 Revision 3 「Digital Identity Guidelines」）

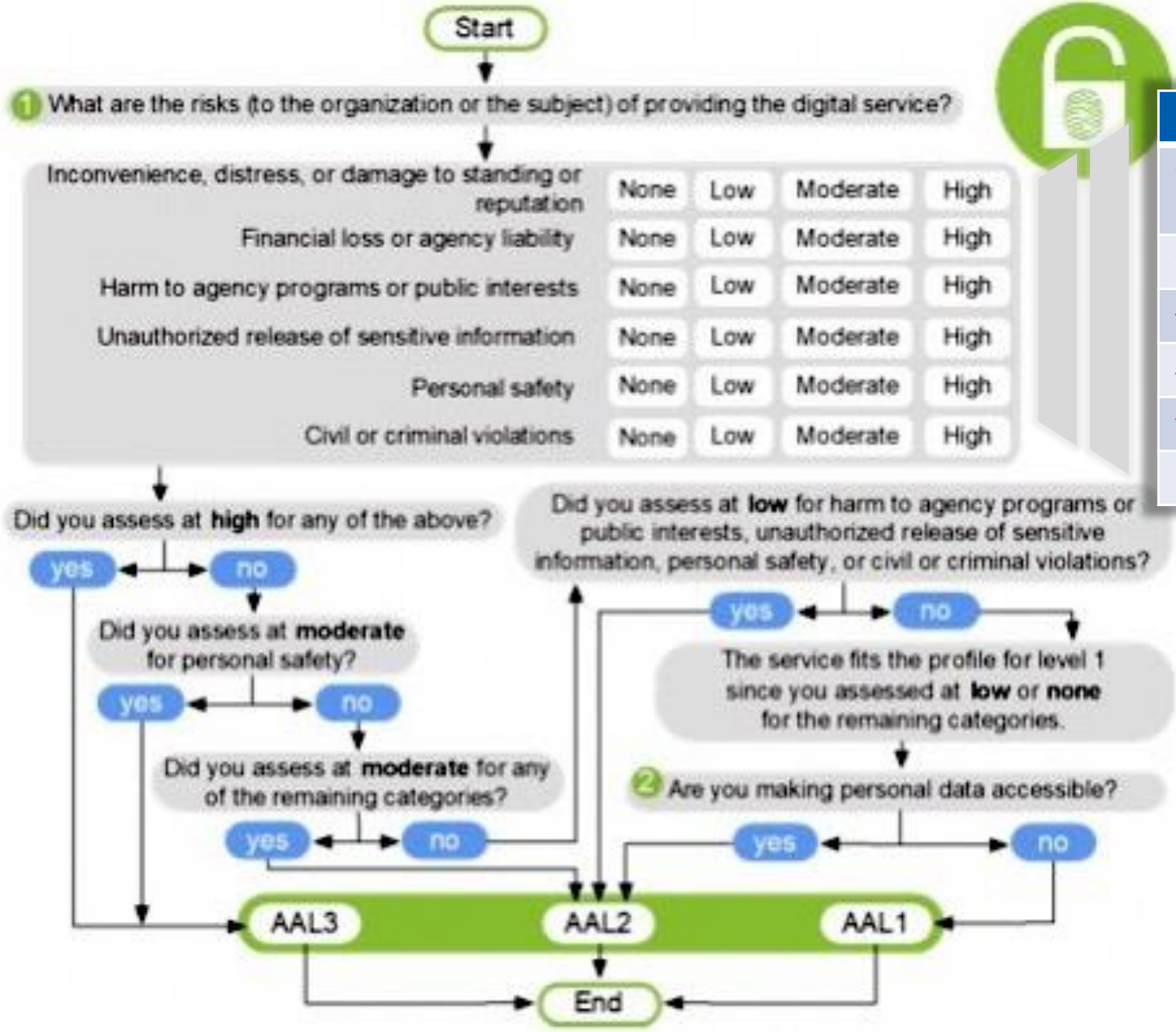


影響のカテゴリー
不便、苦痛、あるいは社会的地位やレピュテーションの毀損
経済的損失または機関の負債
機関のプログラムや公共の利益への損害
Authorizeのないセンシティブ情報の公開
個人の安全
民事または刑事上の違反

「個人の安全」に関する潜在的影響	
None	影響なし
Low	最悪でも、治療を必要としない軽傷
Moderate	最悪でも、軽傷に関する中程度のリスク、ないしは治療を必要とする怪我に関する限定的リスク
High	重大な障害または死亡に関するリスク

（参考）AAL：Authenticationプロセス自体、および Authenticatorと特定個人の識別子の紐付けの頑強性　の選択

（引用元：NIST: National Institute of Standards and Technology Special Publication 800-63 Revision 3 「Digital Identity Guidelines」）



影響のカテゴリー
不便、苦痛、あるいは社会的地位やレピュテーションの毀損
経済的損失または機関の負債
機関のプログラムや公共の利益への損害
Authorizeのないセンシティブ情報の公開
個人の安全
民事または刑事上の違反

「個人の安全」に関する潜在的影響	
None	影響なし
Low	最悪でも、治療を必要としない軽傷
Moderate	最悪でも、軽傷に関する中程度のリスク、ないしは治療を必要とする怪我に関する限定的リスク
High	重大な障害または死亡に関するリスク