参考

米国　EAI（連邦政府認証基盤）に関する補足資料

出典：財団法人日本情報処理開発協会「平成18年度情報基盤対策技術開発等推進費事業（次世代型電子認証基盤の整備）電子認証ポリシーに関する調査報告書」平成19 年3 月
http://www.japanpkiforum.jp/hojo/shiryou/FY2006_report/03_denshi_ninsho_policy_rep.pdf

【項目3の補足表】 リスクカテゴリの例（アメリカEAIの例）

OMBのE-Authentication Guidance for Federal Agenciesでは、誤認証（なりすまし等）がもたらす潜在的なリスクのカテゴリを以下の6つに分類し、カテゴリ毎に3段階の影響度を設定している。

	リスクカテゴリ	影響度		
		Low	Moderate	High
1	不便さ、苦痛、地位や評判への損害	短期間における限定した損害	短期間における深刻な損害、或いは長期間における限定した損害	長期間における深刻或いは非常に厳しい侵害
2	金銭的損失、組織の責務	あまり重要でない、取るにたらない回復不可能な金銭的ロス、或いは組織の責務	深刻な回復不可能な金銭的ロス、或いは組織の責務	非常に厳しい又は壊滅的な金銭的ロス、或いは組織の責務
3	組織計画や公益への被害	組織運用や資産、公益に対して限定されている逆の効果の波及	組織運用や資産、公益に対して深刻な逆の効果の波及	非常に厳しい又は壊滅的な逆の効果の波及
4	センシティブ情報の未許可開示	影響度の低い機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示	影響度が中程度の機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示	影響度の高い機密性損失における個人的、米国政府機密、商業上の機密情報の未許可組織への開示
5	個人の安全	医療措置を必要としない傷害	たいしたことのない傷害の中程度のリスク、或いは医療措置を必要とする限定したリスク	深刻な障害、或いは死のリスク
6	民事上あるいは刑事上の違反	通常は法執行を受けることのない民事上或いは刑事上違反のリスク	法執行を受ける民事上或いは刑事上違反のリスク	法執行計画において非常に重要な民事上或いは刑事上違反のリスク

【項目4の補足表】 リスクカテゴリと認証レベルとのマッピング例（アメリカEAIの例）

OMBの同Guidanceでは、各リスクカテゴリの影響度と認証レベル（認証時に保証すべき信用度のレベル）との対応関係を以下のように示している。カテゴリ毎に決定した認証レベルの中で一番高いものが、対象サービスに必要な認証レベルとなる。

	リスクカテゴリ	（低い←） 認証レベル （→高い）			
		1（アイデンティティの有効性に対する信用度がほとんどない）	2（アイデンティティの有効性に対する信用度がいくらかある）	3（アイデンティティの有効性に対する信用度が高い）	4（アイデンティティの有効性に対する信用度が大変高い）
1	不便さ、苦痛、地位や評判への損害	Low	Mod	Mod	High
2	金銭的損失、組織の責務	Low	Mod	Mod	High
3	組織計画や公益への被害	N/A	Low	Mod	High
4	センシティブ情報の未許可開示	N/A	Low	Mod	High
5	個人の安全	N/A	N/A	Low	Mod High
6	民事上あるいは刑事上の違反	N/A	Low	Mod	High
適用サービス例		・ 教育省"My.ED.gov"カスタマイズページの利用	・連邦政府“Gov Online Learning Center”への会員登録 ・受給者による社会保障Webサイト「住所」の変更	・特許商標局への機密特許情報の電子提出 ・通報者の災害管理報告Webサイトへのアクセス	・捜査当局者の犯罪歴を含むDBへのアクセス ・復員軍事省薬剤師の規制医薬品の調合 ・行政機関調査官のセンシティブな個人情報へのインターネットアクセス

※ 影響度：N/A= Not Available； Low=Low； Mod=Moderate； High=High

※ 認証リスク決定プロセス

1. サービスプロバイダがサービスの認証レベルを決定する際は、まず当該サービスのリスクアセスメントを行い、リスクカテゴリ毎の影響度を導出する。
2. 上記マッピング表によりリスクカテゴリ毎の影響度に対応する認証レベルを各々決定する。
3. リスクカテゴリ毎に決定した認証レベルの中で一番高いものを、対象とするサービスに必要な認証レベルとする。

【項目5の補足表】 認証レベルに対応した基準の例（アメリカEAIの例） 1/5

A. 登録時の本人確認に関する要件

NISTのElectronic Authentication Guidelineでは、認証レベルに応じて直接登録時（対面による登録）とリモート登録時において、RA（登録局）に求める本人確認の要件を以下のように定めている。

	認証レベル	直接登録時の要件	リモート登録時の要件
1	レベル1	要件なし。	要件なし。
2	レベル2	政府機関の発行する写真付きID（住所や国籍付き）。IDの正しさと写真と申込者の一致を確認し、住所の確認が取れたら発行を行う。	政府機関の発行するIDの番号と、金融機関の口座番号。それぞれ該当機関へ照会、名前・生年月日・住所・その他個人情報を確認。住所へ通知を送付するか、住所確認後の発行、又は住所への連絡後発行を行う。
3	レベル3	政府機関の発行する写真付きID。IDについて該当機関へ照会。ID番号・生年月日・住所・その他個人情報を確認。住所を確認後、発行を行う。	政府機関の発行するID番号と金融機関の口座番号。それぞれ該当機関へ照会、名前・生年月日・住所・その他個人情報を確認。住所確認後の発行、又は住所への電話連絡（要録音）後発行を行う。
4	レベル4	Level 3に該当するIDや口座を2つ。一番主要なものは公的な写真付きIDであること。主要なものに関して該当機関へ照会。写真比較、ID番号・生年月日・住所を記録。2つ目に関しては、IDの正しさと写真と申込者の一致を確認、或いは金融機関へ照会し、名前・生年月日・住所・その他個人情報を確認。生体情報を記録（否認防止のため）。住所の確認。以上を終えて初めて発行を行う。	不許可。

【項目5の補足表】 認証レベルに対応した基準の例（アメリカEAIの例） 2/5

B. クレデンシャルの管理に関する要件

NISTの同Guidelineでは、CSP（クレデンシャルサービスプロバイダ）に対して、クレデンシャルの管理に関する要件を以下のように定めている。

	認証レベル	クレデンシャルの有効期限、状態、失効
1	レベル1	（規定なし）
2	レベル2	・CSPはクレデンシャル検証のための安全な仕組みを提供しなければならない。 ・クレデンシャルが利用不可能な状態になってから72時間以内の失効。
3	レベル3	・CSPはクレデンシャル検証のための安全な仕組みを提供しなければならない。 ・クレデンシャルが利用不可能な状態になってから24時間以内の失効。
4	レベル4	・CSPはクレデンシャル検証のための安全な仕組みを提供しなければならない。 ・クレデンシャルが利用不可能な状態になってから24時間以内の失効。 ・機密情報の送信は暗号化され、一時的或いは短時間の暗号鍵の有効期間は24時間以内。

【項目5の補足表】 認証レベルに対応した基準の例（アメリカEAIの例） 3/5

C. 利用可能なトークンに関する要件 （〇は利用可、×は利用不可）

NISTの同Guidelineでは、利用可能なトークンとして、パスワード（又はPIN）トークン、OTPデバイストークン、ソフトウェアトークン、ハードウェアトークンを挙げ、それぞれ強度の観点から技術的要件を規定している。

	認証レベル	パスワード（又はPIN）トークン	OTPデバイストークン	ソフトウェアトークン	ハードウェアトークン
1	レベル1	〇	〇	〇	〇
2	レベル2	〇	〇	〇	〇
3	レベル3	×	〇	〇	〇
4	レベル4	×	×	×	〇

- ソフトウェアトークン：コンピュータや可搬性媒体に格納される暗号鍵。鍵を活性化するためにパスワードまたは生体情報の入力が必要となる（例：PCのハードディスクに格納された電子証明書の暗号鍵（コピー可能））
- ハードウェアトークン：保護された暗号鍵を備えている特定の基準を満たしたハードウェアデバイス。鍵を活性化するためにパスワードまたは生体情報の入力が必要となる（例：PIN入力が必要なICカード）

【項目5の補足表】 認証レベルに対応した基準の例（アメリカEAIの例） 4/5

D. 脅威への耐性に関する要件 （〇は耐性がある）

NISTの同Guidelineでは、認証プロトコルに対する脅威としてオンライン推測攻撃、リプレイ攻撃、盗聴、検証者のなりすまし、中間者攻撃、セッションハイジャックを挙げており、各認証レベルで必要とされる脅威への耐性を以下のように定めている。

	認証レベル	オンライン推測攻撃	リプレイ攻撃	盗聴	検証者のなりすまし	中間者攻撃	セッションハイジャック
1	レベル1	〇	〇				
2	レベル2	〇	〇	〇			
3	レベル3	〇	〇	〇	〇	〇	
4	レベル4	〇	〇	〇	〇	〇	〇

- オンライン推測攻撃：オンラインで何度も認証行為を試みて、パスワード等の認証情報を推測する攻撃
- リプレイ攻撃 ： 前回に利用された正規な認証情報を再現させて、不正に認証させる攻撃
- 盗聴 ： 認証要求者と検証者の間でやり取りされる認証情報を不正に傍受する攻撃
- 検証者のなりすまし ： 攻撃者が正規の検証者を装い、認証情報を不正に取得する攻撃
- 中間者攻撃 ： 攻撃者が認証要求者と検証者の間に介入し、両者間でやり取りされる認証情報を不正に操作（盗聴、改ざん）する攻撃
- セッションハイジャック ： 認証が完了した正規通信（セッションID）を不正に乗っとって、当該通信を悪用する攻撃

【項目5の補足表】 認証レベルに対応した基準の例（アメリカEAIの例） 5/5

E. 利用可能な認証プロトコルに関する要件 （〇は利用可）

NISTの同Guidelineでは、上記の脅威への耐性と関連して、各認証レベルで利用可能な認証プロトコルを以下のように定めている。

	認証レベル	秘密鍵PoP	対称鍵PoP	トンネル化パスワードPoP	チャレンジレスポンスパスワードPoP
1	レベル1	〇	〇	〇	〇
2	レベル2	〇	〇	〇	
3	レベル3	〇	〇		
4	レベル4	〇	〇		

- 秘密鍵PoP：公開鍵暗号方式による認証方式
- 対称鍵PoP：共通鍵暗号方式による認証方式
- トンネル化パスワードPoP：セキュアな（暗号化された）TLSプロトコルセッション（トンネリング）を通じたパスワードによる認証方式
- チャレンジレスポンスパスワードPoP：パスワードとチャレンジの組み合わせによる認証方式