Kantaraの基準(criteria)を調査

- NIST SP 800-63A
  https://pages.nist.gov/800-63-3/sp800-63a.html
  https://openid-foundation-japan.github.io/800-63-3-final/sp800-63a.ja.html
- Kantara Identity Assurance Framework (KIAF)
  https://kantarainitiative.org/?s=KIAF&ct_post_type=post%3Apage%3Aproduct%3Aelementskit_content%3Aelementskit_template%3Aelementskit_widget%3Awpdmpro%3Aigmap%3Ael_events
- 特にKIAF-1430 – Identity Assurance Framework: NIST SP 800-63A Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
  - IAL 2および3が対象

- IAL 3のみに適用される項目は除外
- NIST SP 800-63Aの条文から大きな差分のあるものを抽出
  - 後述

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
2	§	(..)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63A tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience
3	4.2	1	General Requirements	Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.	✓				63A#0010			The CSP SHALL NOT perform identity proofing to determine suitability or entitlement to gain access to services or benefits.	✓	✓		This apparent prohibition need not preclude the collection, at the time of the collection of necessary proofing information, of additional information for post-proofing use so long as that additional information is not used during the proofing process.
	4.2	2	General Requirements	Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation,	✓				63A#0020			The CSP SHALL limit collection of PII to the minimum necessary to validate and resolve the existence of the claimed identity uniquely in a given context, and to associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification.	✓	✓		

KIAF-1430 SP 800-63A SAC & SoCA v4.0

IAL 2のKantara基準を満たすための項目

例

- Privacy Notice
- CrP (Credential Policy)
- CrPS (Credentialing Practices Statement)
- 対面による本人確認
  - one STRONG evidence
  - STRONG validation
  - STRONG verification
- 対面 – UPKIの学術スキーム類似の手法?
- 63Aセクション6 Derived Credentialsによる実現?

以降のスライドはKIAF-1430からの引用

- 4.2 3+ The CSP SHALL explicitly make its Privacy Notice available to the Applicant at the time of collection of the attributes necessary for the Applicant's identity proofing,
- 4.2 5 The CSP SHALL review its redress mechanisms at least every 12 months and assess their efficacy in achieving resolution of complaints or problems, implementing corrective action when efficacy falls below defined thresholds of performance or accomplishment.
- 4.2 6 The CSP SHALL:
- document in a Credential Policy (CrP) its identity proofing and enrollment policy/ies;
- for each type of identity proofing offered (see 63A#0260), state which issuing and authoritative sources are used to prove identities;
- state any eligibility requirements or limitations which it applies to the scope of Applicants to its identity proofing service, subject to such limitations not breaching the restriction placed by 63A#0010;
- publish its CrP such that it is available to members of the intended community (e.g. Applicants, Subscribers, Relying Parties, ...) before they are required to commit to signing-up to being a subject of the policy.
- CrPSも

- 4.4.1.2 3 The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of the evidence it collects satisfies the qualities identified in Table 5-1 [see worksheet 63A_T5-1].
- 4.4.1.3 The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of validation of the evidence it collects satisfies the qualities identified in Table 5-2 [see worksheet 63A_T5-2].
- 4.4.1.4 The CSP SHALL document its justification, for each form of evidence it recognises in fulfilling its CrP and these criteria, of how the strength of verification of the evidence it collects meets, at a minimum, the STRONG qualities identified in Table 5-3 [see worksheet 63A_T5-3].
- 4.4.1.5 The CSP SHALL offer at least one of the following types of identity proofing and SHALL clearly state in its CrP which of those types it provides, describing clearly how requirements between multiple identity proofing types differ.
- Supervised (In-person);
- Supervised (Remote);
- Unsupervised.
- 4.4.2 CSPs SHALL identity-proof Trusted Referees according to the same criteria and, as a minimum, at the same IAL that are applied to normal Applicants on whose behalf they act.

- 5.3.3.1 1 If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures which ensure that the Proofing Supervisor reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.
- 5.3.3.1 2 If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures such that the Proofing Supervisor SHALL ensure that biometric samples are taken from the Applicant themselves and not from another person.
- If the CSP provides Supervised (In-person) proofing it SHALL ensure that the technologies and procedures applied by the Proofing Supervisor fulfill the biometric performance requirements expressed in 63A#0620 to 63A#0680 inclusive.

NIST SP 800-63A Table 5-1 Strengths of Identity Evidence

Strength	63A tag	indx			KI_criterion
FAIR	63A-T5-1#fair	a)			The CSP can demonstrate or show other reasonable expectation that the Issuing Source of the evidence:
	63A-T5-1#fair	a)	i)		confirmed the claimed identity through an identity proofing process;
	63A-T5-1#fair	a)	ii)		delivered the evidence into the possession of the person to whom it relates.
	63A-T5-1#fair	b)			The evidence collected by the CSP:
	63A-T5-1#fair	b)	i)		Contains at least one reference number that uniquely identifies the person to whom it relates; OR
	63A-T5-1#fair	b)	ii)		Contains a photograph or biometric template (any modality) of the person to whom it relates; OR
	63A-T5-1#fair	b)	iii)		Can have ownership confirmed through KBV.
	63A-T5-1#fair	c)			Where the evidence collected by the CSP includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	63A-T5-1#fair	d)			Where the evidence collected by the CSP includes physical security features, it requires proprietary knowledge to be able to reproduce those features.
	63A-T5-1#fair	e)			The evidence collected by the CSP is unexpired.
STRONG	63A-T5-1#strg	a)			The CSP can demonstrate or show other reasonable expectation that the Issuing Source of the evidence:
	63A-T5-1#strg	a)	i)		confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the Applicant.
	63A-T5-1#strg	a)	ii)		has its written procedures subjected to recurring oversight by regulatory or publicly-accountable institutions;
	63A-T5-1#strg	a)	iii)		delivered the evidence into the possession of the subject to whom it relates.
	63A-T5-1#strg	b)			The evidence collected by the CSP contains at least one reference number that uniquely identifies the person to whom it relates and to the Issuing Source.
	63A-T5-1#strg	c)			The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names.
	63A-T5-1#strg	d)			Either the:
	63A-T5-1#strg	d)	i)		evidence collected by the CSP contains a photograph or biometric template (of any modality) of the person to whom it relates, OR
	63A-T5-1#strg	d)	ii)		Applicant proves possession of an AAL2 authenticator bound to an IAL2 identity, at a minimum.
	63A-T5-1#strg	e)			Where the evidence collected by the CSP includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.
	63A-T5-1#strg	f)			Where the evidence collected by the CSP contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it.
	63A-T5-1#strg	g)			The evidence collected by the CSP is unexpired.
SUPERIOR	63A-T5-1#supr	a)			It can be demonstrated that the issuing source of the evidence:
		a)	i)		confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the applicant;
		a)	ii)		has its written procedures subjected to recurring oversight by regulatory or publicly-accountable institutions;
		a)	iii)		visually identified the applicant and performed further checks to confirm the existence of that person;
		b)			employed processes which ensured that the evidence was delivered into the possession of the person to whom it relates.
		c)			The evidence collected by the CSP contains at least one reference number that uniquely identifies the person to whom it relates and to the issuing source.
		d)			The full name on the evidence collected by the CSP is the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names.
		e)			The evidence collected by the CSP contains a photograph of the person to whom it relates.
		f)			The evidence collected by the CSP contains a biometric template (of any modality) of the person to whom it relates.
		g)			The evidence collected by the CSP includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed.
		h)			The evidence collected by the CSP includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it.
		i)			The evidence collected by the CSP is unexpired.

NIST SP 800-63A Table 5-2 Validating Identity Evidence					
Strength	63A tag	indx			KI_criterion
FAIR	63A-T5-2#fair	a)			The CSP can demonstrate that the evidence which it has collected:
	63A-T5-2#fair	a)	i)		has attributes confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s); OR
	63A-T5-2#fair	a)	ii)		has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified; OR
	63A-T5-2#fair	a)	iii)		has been confirmed as genuine by trained personnel; OR
	63A-T5-2#fair	a)	iv)		has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
STRONG	63A-T5-2#strg	a)			The CSP can demonstrate that the evidence which it has collected has been confirmed as genuine:
	63A-T5-2#strg	a)	i)		using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified; OR
	63A-T5-2#strg	a)	ii)		by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified; OR
	63A-T5-2#strg	a)	iii)		by confirmation of the integrity of cryptographic security features.
	63A-T5-2#strg	b)			The CSP can demonstrate that the evidence which it has collected has had all personal details and evidence details confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
SUPERIOR	63A-T5-2#supr	a)			The CSP can demonstrate that the evidence which it has collected has been confirmed as genuine by trained personnel and the use of appropriate technologies, including the integrity of any physical and cryptographic security features;
	63A-T5-2#supr	b)			The CSP can demonstrate that the evidence which it has collected has had all personal details and evidence details confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

NIST SP 800-63A Table 5-3 Verifying Identity Evidence					
Strength	63A tag	indx			KI_criterion
FAIR	n/a				
Not applicable since 'FAIR' verification is not permissable at IAL2 (§ 4.4.1.4 1))	n/a				
	n/a				
	n/a				
STRONG	63A-T5-3#strg	a)			The CSP SHALL confirm the Applicant's ownership of the claimed identity by:
	63A-T5-3#strg	a)	i)		a physical comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all criteria 63A#0620 to 63A#0680 inclusive; OR
	63A-T5-3#strg	a)	ii)		biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all criteria 63A#0620 to 63A#0680 inclusive.
SUPERIOR	63A-T5-3#supr	a)			The CSP SHALL confirm the Applicant's ownership of the claimed identity by biometric comparison of the Applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all criteria 63A#0620 to 63A#0680 inclusive.