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+ CSPは、ApplicantのIdentity Proofingに必要なAttributeの収集時に、ApplicantがPrivacy Noticeを明示的に利用できるようにする（SHALL）。
- 4.2 5 CSPは、少なくとも12か月ごとにその是正メカニズムを見直し、苦情や問題の解決を達成する上での有効性を評価し、有効性がパフォーマンスまたは達成の目安として定義されたものを下回った場合には是正措置を実施する（SHALL）。
- 4.2 6 CSPは以下を行う（SHALL）。
- Credential Policy（CrP）のなかで、Identity ProofingおよびEnrolmentのポリシーを文書化する。
- 提供されたIdentity Proofingのタイプごとに（63A#0260を参照）、Identityを証明する上で、どのIssuing SourceおよびAuthoritative Sourceが使用されているかを述べる。
- 63A#0010に課された制限に反しないという制約を条件として、そのIdentity Proofingサービスへの Applicantの範囲に適用される資格要件または制限を述べる。
- ポリシーの対象となるために署名することを求める前に、意図されたコミュニティのメンバー（Applicant, Subscriber, Relying Partyなど）が利用できるようにCrPを公開する。
- CrPSも

- 4.4.1.2 3 CSPは、そのCrPやこれらの基準を満たす上で認識し収集したエビデンスの各形式について、また、収集したエビデンスの強度が表5-1に特定された品質をどのように満たしているかについて、その正当性を文書化する（SHALL）[worksheet 63A_T5-1を参照のこと]。
- 4.4.1.3 CSPは、そのCrPやこれらの基準を満たす上で認識し収集したエビデンスの各形式について、また、収集したエビデンスの検証の強度が表5-2に特定された品質をどのように満たしているかについて、その正当性を文書化する（SHALL）[worksheet 63A_T5-2 を参照のこと]。
- 4.4.1.4 CSPは、そのCrPやこれらの基準を満たす上で認識し収集したエビデンスの各形式について、また、収集したエビデンスの検証の強度が、少なくとも表5-3に特定されたSTRONG品質をどのように満たしているかについて、その正当性を文書化する（SHALL）[worksheet 63A_ T5-3を参照のこと]。
- 4.4.1.5 CSPは、次のタイプのIdentity Proofingを少なくとも1つ提供し（SHALL）、かつ、CrPの中で複数のIdentity Proofingのタイプ間の要件がどのように異なるかを記述し、これらのどのタイプを提供するのかを明確に示す（SHALL）。
  監視下(対面);
  監視下（Remote）；
  非監視下。
- 4.4.2 CSPは、Applicantの代理として行動するTrusted RefereesのIdentity Proofingを、同じ基準、および、少なくとも、通常のApplicantに適用されるのと同じIALに従って行う（SHALL）。

- 5.3.3.1 1 CSPが監視下の（対面）Proofingを提供する場合は、Proofing SupervisorがBiometric 情報源（指、顔など）に非天然物質が存在するかを確認し、Proofing プロセスの一部としてそのような検査を行うように、技術と手順を文書化し、適用する（SHALL）。
- 5.3.3.1 2 CSPが監視下の（対面）Proofingを提供する場合は、Proofing SupervisorがBiometric サンプルが他人からではなく当該Applicantから取得されるように、技術と手順を文書化し、適用する（SHALL）。
- CSPが監視下の（対面）Proofingを提供する場合は、Proofing Supervisorが適用する技術と手順が、63A#0620から63A#0680までに示されているBiometric Performance要件を満たしているようにする（SHALL）。

Table 5-1 Strengths of Identity Evidence

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

Strength	63A tag	indx		KI_criterion
FAIR	63A-T5-1#fair	a)		CSPは、当該エビデンスのIssuing Sourceが次のことを行うという、その他の合理的な期待を示すことができる。
	63A-T5-1#fair	a)	i)	Identity Proofingプロセスを通じてClaimed Identityを確認している。
	63A-T5-1#fair	a)	ii)	当該エビデンスがそれに紐づく人物の管理下に送達された。
	63A-T5-1#fair	b)		CSPによって収集されたエビデンスが：
	63A-T5-1#fair	b)	i)	紐づいている人物を一意に識別できる、少なくとも1つの参照番号を含む。OR
	63A-T5-1#fair	b)	ii)	紐づいている人物の写真もしくは Biometricテンプレート（様式は問わない）を含む。OR
	63A-T5-1#fair	b)	iii)	KBVを通じて所有権の確認が可能。
	63A-T5-1#fair	c)		CSPによって収集されたエビデンスにデジタル情報が含まれる場合、その情報は承認された暗号化や独自の（proprietary） 方法、または、その両方により保護され、これらの方法により、情報の Integrity が確保され、Claimed Issuing Source の Authenticity が確認できる。
	63A-T5-1#fair	d)		CSPによって収集されたエビデンスに物理的セキュリティ機能が含まれる場合、それを再現するには独自の（proprietary）の知識が必要である。
	63A-T5-1#fair	e)		CSPによって収集されたエビデンスは期限切れしていない。
STRONG	63A-T5-1#strg	a)		CSPは、当該エビデンスのIssuing Sourceが次のことを行うという、その他の合理的な期待を示すことができる。
	63A-T5-1#strg	a)	i)	Applicantの現実世界のIdentity について合理的な確信を持てるように設計された文書化された手続きを通じて、Claimed Identity を確認している。
	63A-T5-1#strg	a)	ii)	このような書面による手続きが、規制当局または公的に責任がある機関によって定期的に監督されている。
	63A-T5-1#strg	a)	iii)	当該エビデンスがそれに紐づく Subject の管理下に送達された。
	63A-T5-1#strg	b)		CSPによって収集されたエビデンスに、それに紐づく人物を一意に識別できる、少なくとも1つの参照番号が含まれている。
	63A-T5-1#strg	c)		当該エビデンスに記載されたフルネームは、発行時点において当人にオフィシャルに認識されている名前でなければならない。仮名、エイリアス、名字のイニシャル、すべての名前のイニシャルなどは許容されない。
	63A-T5-1#strg	d)		いずれか：
	63A-T5-1#strg	d)	i)	当該エビデンスが、それに紐づいている人物の写真もしくは Biometricテンプレート（様式は問わない）を含む。OR
	63A-T5-1#strg	d)	ii)	Applicant が、最低限 IAL2 の Identity に紐づいた AAL2 の Authenticator を保持していることを証明する。
	63A-T5-1#strg	e)		CSPによって収集されたエビデンスにデジタル情報が含まれる場合、その情報は承認された暗号化や独自の（proprietary）方法、または、その両方により保護され、これらの方法により、情報の Integrity が確保され、Claimed Issuing Source の Authenticity が確認できる。
	63A-T5-1#strg	f)		CSPによって収集されたエビデンスに物理的セキュリティ機能が含まれる場合、それを再現するには独自の（proprietary）の知識が必要である。
	63A-T5-1#strg	g)		CSPによって収集されたエビデンスは期限切れしていない。
SUPERIOR	63A-T5-1#supr	a)		当該エビデンスのIssuing Sourceが次を行うということを示すことができる。
		a)	i)	SourceがApplicantの現実世界のIdentity について高い確信を持てるように設計された文書化された手続きを通じて、Claimed Identity を確認している。
		a)	ii)	その書面による手続きが、規制当局または公的に責任がある機関によって定期的に監督されている。
		a)	iii)	Applicant を視覚的に識別し、当人の存在確認のためのさらなるチェックを行なった。
		b)		当該エビデンスがそれに紐づく人物の管理下に送達されるような手順を採用した。
		c)		CSPによって収集されたエビデンスに、それに紐づく人物とIssuing Sourceを一意に識別できる、少なくとも1つの参照番号が含まれている。
		d)		CSPによって収集されたエビデンスに記載されたフルネームは、発行時点において当人にオフィシャルに認識されている名前でなければならない。仮名、エイリアス、名字のイニシャル、すべての名前のイニシャルなどは許容されない
		e)		CSPによって収集されたエビデンスは、それに紐づいている人物の写真を含む。
		f)		CSPによって収集されたエビデンスは、それに紐づいている人物のBiometricテンプレート（様式は問わない）を含む。
		g)		CSPによって収集されたエビデンスにデジタル情報が含まれる場合、その情報は承認された暗号化や独自の（proprietary）方法、または、その両方により保護され、これらの方法により、情報の Integrity が確保され、Claimed Issuing Source の Authenticity が確認できる。
		h)		CSPによって収集されたエビデンスに物理的セキュリティ機能が含まれる場合、それを再現するには独自の（proprietary）の知識と独自の（proprietary）の技術が必要である。
		i)		CSPによって収集されたエビデンスは期限切れしていない。

Table 5-2 Validating Identity Evidence

NIST SP 800-63A Table 5-2 Validating Identity Evidence					
Strength	63A tag	indx			KI_criterion
FAIR	63A-T5-2#fair	a)			CSPは、収集したエビデンスが次であることを示すことができる。
	63A-T5-2#fair	a)	i)		Attribute について、Issuing SourceまたはAuthoritative Source が保有ないしは公開している情報と比較して正当性が確認されている。OR
	63A-T5-2#fair	a)	ii)		適切な技術を使用して、物理的セキュリティ機能の Integrity が確認され、当該エビデンスが不正または不適切に改ざんされておらず、本物であることが確認されている。OR
	63A-T5-2#fair	a)	iii)		訓練を受けた担当者により、本物であることが確認されている。OR
	63A-T5-2#fair	a)	iv)		暗号化セキュリティ機能の Integrity が確認され、本物であることが確認されている。
STRONG	63A-T5-2#strg	a)			CSPは、収集したエビデンスが本物であることが確認されていることを示すことができる。
	63A-T5-2#strg	a)	i)		適切な技術を使用して、物理的セキュリティ機能の Integrity が確認され、当該エビデンスが不正または不適切に改ざんされていないことが確認されている。OR
	63A-T5-2#strg	a)	ii)		訓練を受けた担当者と適切な技術により、物理的セキュリティ機能の Integrity が確認され、当該エビデンスが不正または不適切に改ざんされていないことが確認されている。OR
	63A-T5-2#strg	a)	iii)		暗号化セキュリティ機能の Integrity が確認されている。
	63A-T5-2#strg	b)			CSPは、収集したエビデンスのすべての個人情報とエビデンスに関する詳細について、Issuing Source または Authoritative Source が保有ないしは公開している情報と比較して正当性が確認されていることを示すことができる。
SUPERIOR	63A-T5-2#supr	a)			CPSは、収集したエビデンスが、訓練を受けた担当者、および、物理的セキュリティと暗号的セキュリティ機能の Integrity を含む適切な技術の使用によって、本物であることが確認されていることを示すことができる。
	63A-T5-2#supr	b)			CPSは、収集したエビデンスのすべての個人情報とエビデンスに関する詳細について、Issuing Source または Authoritative Source が保有ないしは公開している情報と比較して正当性が確認されていることを示すことができる。

Table 5-3 Verifying Identity Evidence

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)			CSPは、次の方法で、Applicant が Claimed Identity の所有者であることを確認する（SHALL）。
	63A-T5-3#strg	a)	i)		Applicant と、Claimed Identity を裏付けるために提示されたものの中でもっとも強度の高い Identity Evidence との物理的な比較。Remoteで物理的比較を行なう際は、63A#0620から63A#0680までのすべての基準に準拠していること（SHALL）。OR
	63A-T5-3#strg	a)	ii)		Applicant と Identity Evidence の Biometricの比較。Remote で Biometric 比較を行なう際は、63A#0620から63A#0680までのすべての基準に準拠していること（SHALL）。
SUPERIOR	63A-T5-3#supr	a)			CSPは、適切な技術を使用して、Applicant と、Claimed Identity を裏付けるために提示されたものの中でもっとも強度の高い Identity Evidence とのBiometric 比較を行なうことにより、Applicant が Claimed Identity の所有者であることを確認する（SHALL）。Remote で Biometric 比較を行なう際は、63A#0620から63A#0680までのすべての基準に準拠していること（SHALL）。