AAL2 - Kantaraの基準(criteria)を調査

- NIST SP 800-63B
  https://pages.nist.gov/800-63-3/sp800-63b.html
  https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.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-1440 – Identity Assurance Framework: NIST SP 800-63B Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
  - AAL 2および3が対象

Kantara基準Excelのフォーマットについて

- 真ん中のKI_criterionに記述がある（和訳あり）
- AAL 3のみに適用される項目は除外

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
1	NIST SP 800-63B (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 Assessm							CRITERION APPLICABILITY (So	Guidance	
2	§	(···)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	KI_基準 (赤字の箇所が本文書による最新版)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	注:ガイダンスは、KI-IAWGメンバー追加される
4	4		Authenticator Assurance Levels	To satisfy the requirements of a given AAL, a claimant SHALL be authenticated with at least a given level of strength to be recognized as a subscriber.	✓				63B#0010			The CSP SHALL authenticate a Claimant at at least the ~~same~~ requested AAL.	CSPは、少なくとも~~同じ~~要求された AAL でClaimantを認証する（SHALL）。	✓	✓		This requires that the Claimant must have been issued with and be in possession of a Credential of the same level or higher than that which has been requested before the CSP can consider subjecting the Claimant to an authentication process. The table below considers the acceptability for authentication processing of all AAL1/2/3 combinations. Requested AAL / Lowest Cred AAL / Min Authn AAL which can be attempted 1 / 1 / 1 (Note - IAL1 / AAL1 1 / 2 / 2 are not supported 1 / 3 / 3 by Kantara) 2 / 1 / No Authn permissible 2 / 2 / 2 2 / 3 / 3 3 / 1 / No Authn permissible 3 / 2 / No Authn permissible 3 / 3 / 3	これには、CSPがClaimantに認証に、Claimantが要求されたものとれ、所有していなければならないプロセスのAAL1/2/3の全組み合わ要求される 最低限Cred 試行可 AAL AAL 1 1 1 2 1 3 2 1 2 2 2 3 3 1 3 2 3 3
	4		Authenticator Assurance Levels	The result of an authentication process is an identifier that SHALL be used each time that subscriber authenticates to that RP	✓				63B#0020			The CSP SHALL ensure that, for a given Subject and authenticator, the result of a successful authentication results in a consistent identifier	CSPは、特定のSubjectとAuthenticatorについて、認証が成功した結果、一貫した識別子が得られることを確認する（SHALL）。	✓	✓			

KIAF-1440 SP 800-63B SAC & SoCA v4.0

認証器(Authenticator)の種類

- Multi-Factor Authenticatorを使用する場合、CSPは次のいずれかを使用する（SHALL）。
  - Multi-Factor OTPデバイス、
  - Multi-Factor 暗号化ソフトウェア、
  - Multi-Factor 暗号化デバイス。
- 2つのSingle-Factor Authenticatorの組み合わせを使用する場合、CSPは、Memorized Secret Authenticatorと、次のPossession-Based Authenticatorのいずれか一つを使用する（SHALL）。
  - Look-Up Secret、
  - 帯域外デバイス、
  - Single-Factor OTPデバイス、
  - Single-Factor暗号化ソフトウェア、
  - Single-Factor 暗号化デバイス。

考慮点

- *CSPは、認証プロセスで使用されるデバイスのロック解除をAuthentication Factorと見なさない（SHALL NOT）。*
- *RPは、SubjectのAffirmativeな再認証を受信できない場合には常に、Sessionと現在のSession Secretの有効期間を終了する（SHALL）。*
  - *a）Sessionの非アクティブ期間が30分に達する前、または（OR）*
  - *b）ユーザーのアクティビティに関係なく、最後に成功した再認証から12時間に達する延長使用Sessionの前。*
- *CSPは、以下を考慮しつつ、Data Retention Scheduleを文書化し、定期的に見直し、遵守する（SHALL）。*
  - *Privacy and Security Risk Assessmentの結果、*
  - *適用される法律、規制、ポリシー、および特定のRecord Retention Schedule、*
  - *独自のRecord Retention Schedule。*
- *CSPは、Subjectから Authenticatorの紛失または盗難が疑われる旨の通知があった場合、直ちにAuthenticatorを取り消すか一時停止するための文書化されたメカニズムを提供する（SHALL）。*
- *その他、Memorized Secretの要件等*

Clause titles

- Authenticator Assurance Levels
- Authenticator Assurance Level 2
- Permitted Authenticator Types
- Authenticator and Verifier Requirements
- Reauthentication
- Security Controls
- Records Retention Policy
- Privacy Requirements
- Memorized Secret Authenticators
- Memorized Secret Verifiers
- Look-Up Secrets
- Look-Up Secret Authenticators
- Look-Up Secret Verifiers
- Out-of-Band Authenticators
- Out-of-Band Verifiers
- Authentication using the Public Switched Telephone Network
- Single-Factor OTP Device
- Single-Factor OTP Authenticators
- Single-Factor OTP Verifiers
- Multi-Factor OTP Devices
- （中略）
- Physical Authenticators
- Rate Limiting (Throttling)
- Use of Biometrics
- Attestation
- Verifier-CSP Communications
- Verifier-Compromise Resistance
- Authentication Intent
- Restricted Authenticators
- Authenticator Binding
- Binding at Enrollment
- Binding of an Additional Authenticator at Existing AAL
- Replacement of a Lost Authentication Factor
- Binding to a Subscriber-provided Authenticator
- Loss, Theft, Damage, and Unauthorized Duplication
- Expiration
- Revocation and Termination
- Reauthentication
- Reauthentication from a Federation or Assertion