「学認技術運用基準」新旧対照表（v2.5:v2.6）

新旧対照表の備考欄の記述の意味は以下のとおり。

変更点 A：WTCA という略称を用いている箇所に正式名称を挿入
変更点 B：スコープに関する制約を属性情報仕様一覧から 8.3)に移動
　　変更：その他の既存の文言を変更したもの
　　修正：不要な改行等を修正したもの

V2.5	V2.6	備考
2.3)　Shibboleth Shibboleth は、Shibboleth Consortium(http://shibboleth.net)が開発、提供する SAML をベースとするソフトウェアである。 ・ Shibboleth Identity Provider 3（https://wiki.shibboleth.net/confluence/display/IDP30/Home ）、 Shibboleth Service Provider 3（https://wiki.shibboleth.net/confluence/display/SP3/Home）およびそれ以降 - IdP は 3.4.0 以上、SP は 3.0.0 以上を推奨. ただし、海外 SP 等のサービスを利用することを目的として、SAML1 プロトコルおよび Shibboleth1.3 プロトコルを利用してもよい。	2.3)　Shibboleth Shibboleth は、Shibboleth Project / Consortium (http://shibboleth.net)が開発、提供する SAML をベースとするソフトウェアである。 ・Shibboleth Identity Provider 4（https://wiki.shibboleth.net/confluence/display/IDP4/Home)、Shibboleth Service Provider 3（https://wiki.shibboleth.net/confluence/display/SP3/Home）およびそれ以降 - IdP は 4.0.1 以上、SP は 3.2.0 以上を推奨. ただし、海外 SP 等のサービスを利用することを目的として、SAML1 プロトコルおよび Shibboleth1.3 プロトコルを利用してもよい。	変更 修正 変更
7.4)　信頼する証明書 各エンティティが XML 署名や XML 暗号化、TLS 相互認証を行うための証明書は、その信頼性を担保するために、以下に掲げる条件を満たさなければならない。なお、ここで「エンティティにマッチする」とは、当該エンティティのメタデータに含まれる entityID 、 <SingleSignOnService>、<AssertionConsumerService>に示されるエンドポイントのいずれかのドメイン名が、当該証明書において RFC 6125 に規定され	7.4)　信頼する証明書 各エンティティが XML 署名や XML 暗号化、TLS 相互認証を行うための証明書は、その信頼性を担保するために、以下に掲げる条件を満たさなければならない。なお、ここで「エンティティにマッチする」とは、当該エンティティのメタデータに含まれる entityID 、 <SingleSignOnService> 、<AssertionConsumerService>に示されるエンドポイントのいずれかのドメイン名が、当該証明書において RFC 6125 に規定された検証をパスすることをいう。ただし、IdP に	修正

た検証をパスすることをいう。ただし、IdPにおいては上記いずれも自機関・組織もしくは機関の組織の場合は組織を包含する機関が所有するドメインでない場合は、 3.5)に定めるスコープと一致するドメイン名もしくは当該ドメイン配下の任意のドメイン名が上記検証をパスする場合も「エンティティにマッチする」とみなし、同条件ではこのような証明書を用いることが推奨される。ただしこの場合、証明書の更新では原則として同一のドメイン名を用いるものとする。 －国立情報学研究所 UPKI 証明書発行サービスにより発行された証明書で、エンティティにマッチするもの https://certs.nii.ac.jp/（サービス案内ウェブページ） －WTCA に準拠した認証局、かつ委員会が認めた認証局から発行された証明書で、エンティティにマッチするもの －上掲の要件を満たす別の証明書を利用する Web サイトに配置することによって、当該エンティティとの紐付けが確認できた証明書 －大学のキャンパス認証局等のローカル認証局、かつ委員会が認めた認証局から発行された証明書で、エンティティにマッチするもの －現に他国のフェデレーションに参加しているエンティティであって、運用上の制約により上掲の要件を満たす証明書が利用できないと認められる場合において、入手手段を含め委員会が認めた証明書 －その他委員会が特に認めた証明書 なお、失効した証明書は使用すべきではない。また、証明書は 3 年を目処に定期的に更新すべきである。	おいては上記いずれも自機関・組織もしくは機関の組織の場合は組織を包含する機関が所有するドメインでない場合は、3.5)に定めるスコープと一致するドメイン名もしくは当該ドメイン配下の任意のドメイン名が上記検証をパスする場合も「エンティティにマッチする」とみなし、同条件ではこのような証明書を用いることが推奨される。ただしこの場合、証明書の更新では原則として同一のドメイン名を用いるものとする。 －国立情報学研究所 UPKI 証明書発行サービスにより発行された証明書で、エンティティにマッチするもの https://certs.nii.ac.jp/（サービス案内ウェブページ） － WebTrust for Certification Authorities (WTCA)に準拠した認証局、かつ委員会が認めた認証局から発行された証明書で、エンティティにマッチするもの －上掲の要件を満たす別の証明書を利用する Web サイトに配置することによって、当該エンティティとの紐付けが確認できた証明書 －大学のキャンパス認証局等のローカル認証局、かつ委員会が認めた認証局から発行された証明書で、エンティティにマッチするもの －現に他国のフェデレーションに参加しているエンティティであって、運用上の制約により上掲の要件を満たす証明書が利用できないと認められる場合において、入手手段を含め委員会が認めた証明書 －その他委員会が特に認めた証明書 なお、失効した証明書は使用すべきではない。また、証明書は 3 年を目処に定期的に更新すべきである。	変更点 A

8.3）　ID 利用者の同一性の保証 前項における再利用の場合を除いて、IdP では、同一 ID でのアクセスが同一人物からによることを保証するための方策を講じなければならない。	8.3）　ID 利用者の同一性の保証 前項における再利用の場合を除いて、IdP では、同一 ID でのアクセスが同一人物からによることを保証するための方策を講じなければならない。さらに同一のスコープを複数の IdP で用いている場合は、eduPersonPrincipalName 等スコープ付きの ID 属性について、当該スコープを共用する全ての IdP の中で共通する各 ID でのアクセスが同一人物からによることを保証するための方策を講じなければならない。	変更点 B
5. eduPersonPrincipalName 説明等 フェデレーション内で一意な、かつ、永続的な利用者識別子。「スコープ内で一意な利用者識別子」とスコープを合わせることで、フェデレー ション内での一意性を保証します。IdP は、フェデレーションに参加しこの属性を送信するよう設定した全ての SP に対して、同一の ID であれば同じ値を送信します。 なお、属性値のローカルパート部に「@」を含めることはできません。また、特に同一のスコープを複数の IdP で用いている場合は別人に同じ識別子が割り当てられないようにするべきです。 設定例：t-ninsyo2009@b-univ.ac.jp	5. eduPersonPrincipalName 説明等 フェデレーション内で一意な、かつ、永続的な利用者識別子。「スコープ内で一意な利用者識別子」とスコープを合わせることで、フェデレー ション内での一意性を保証します。IdP は、フェデレーションに参加しこの属性を送信するよう設定した全ての SP に対して、同一の ID であれば同じ値を送信します。 なお、属性値のローカルパート部に「@」を含めることはできません。 設定例：t-ninsyo2009@b-univ.ac.jp	変更点 B