

OpenID Foundation Japan + 学認 学生IDを利用したトラストフレームワーク (SITF) の紹介

ニッポンクラウドワーキンググループ 第八回会合

2012年7月2日

ソフトバンクBB/ソフトバンクテレコム 小松 隆行

■ ホワイトクラウド 仮想サーバ よろしくお願ひします

https://tm.softbank.jp/business/white_cloud/iaas/virtual_server/

iaaS サーバリソース ▶ iaaS 一覧に戻る

仮想サーバ

▶ オンライン申込

概要 詳細 基本サービス オプションサービス 料金案内 よくあるご質問

- 仮想サーバを業界トップレベルの低価格でご提供

※ 「シェアードHaaSスタンダード」は、2012年3月をもちまして「仮想サーバ」へ名称変更を行いました。

月額 **5,250円** /VM～

オンラインサインナップで
あっという間に利用可能!

▶ お申し込みはこちら

「ホワイトクラウド 仮想サーバ」は、オープンソースを用いた通信キャリアならではの高品質、高セキュリティサービスです。加えて、仮想化技術によるハードウェアの効率的な利用やソフトバンクグループの調達力により、安価な価格設定を実現しています。

特長

- ・ 国内データセンター利用による低い伝送遅延
- ・ 日本語による申し込み、問い合わせ、サポート
- ・ 日本国内法に準拠
- ・ 設定変更が簡単な管理ポータルを提供

- ソフトバンクテレコム クラウドサービス開発本部 所属
 - ホワイトクラウド 仮想サーバ システム担当

- ソフトバンクBB 情報システム本部 所属
 - OpenID ファウンデーション・ジャパン 会員 (Since 2008)

■ OpenID 2.0 Authentication (Since 2007/12)

- ユーザ自身がIDを選べる/たくさんのID/パスワードを使い分ける必要がなくなる
- 2012年現在、国内ビジネスユースでは意外と普及している

■ OAuth

- ソーシャルウェブ以後のインターネットサービスで爆発的に普及
- 第三者に対してAPI利用権限を委譲するプロトコル (≠ユーザ認証プロトコル)
- OAuthでユーザ認証を行う事例が多発 (twitter/facebook でログイン)
- OI DF 会長 崎村さんのブログ:「単なる OAuth 2.0 を認証に使うと、車が通れるほどのどでかいセキュリティ・ホールができる」 <http://www.sakimura.org/2012/02/1487/>

■ OpenID Connect

- OAuth2.0の拡張仕様
- API利用のアクセストークンとは別のIDトークンで認証管理

※ OpenID ファウンデーション・ジャパン

- 日本国内での「OpenID」関連技術の普及・啓蒙を行っております
- <http://www.openid.or.jp/>

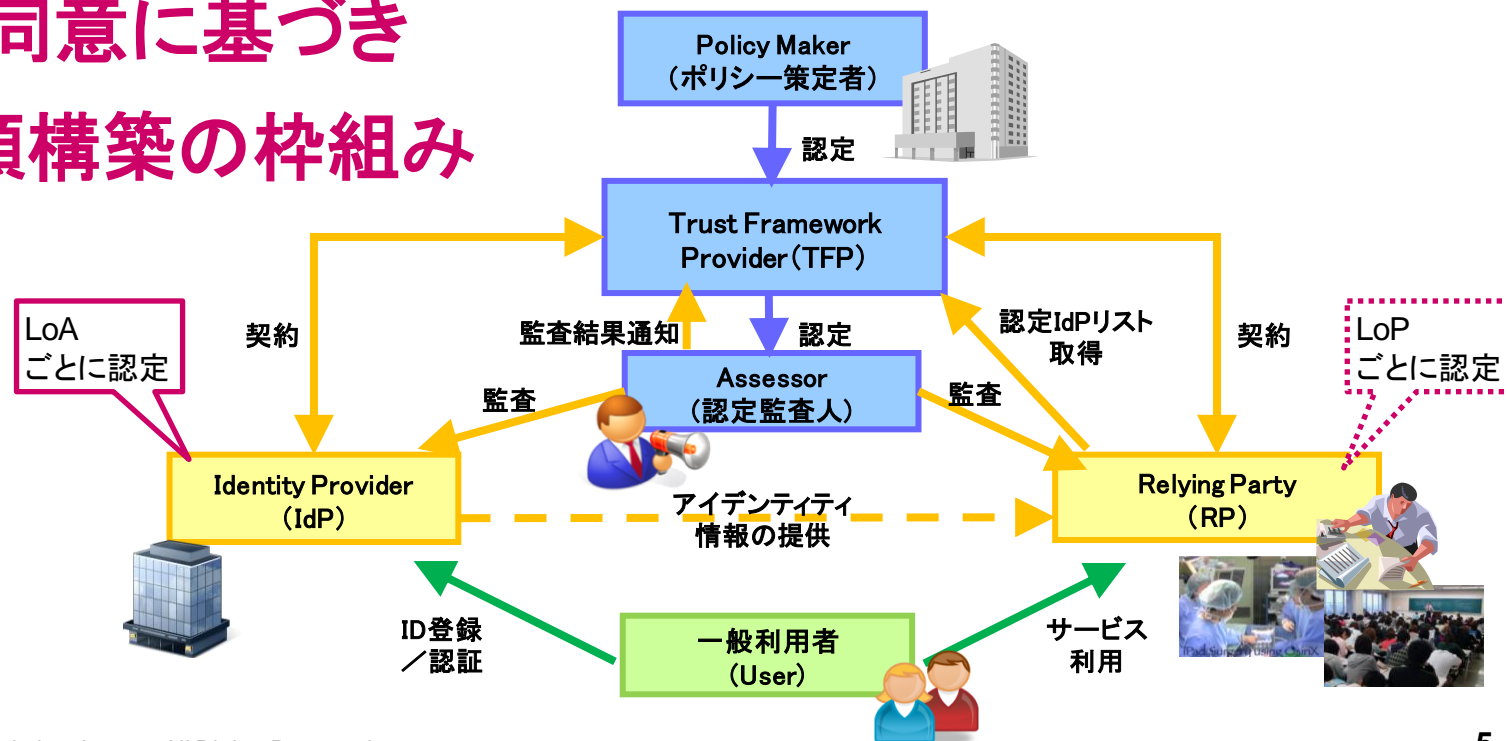
- 民間企業のIDを民間企業が利用する際の信頼性を担保するための枠組みが必要
 - 属性情報が正しく流通し、それが信頼でき・正しい情報であることが保証されれば、ソーシャルウェブの世界に留まらずビジネスユースでもいろいろなことが実現できそう。

- Trust Frameworkに関する世界的な潮流
 - 米国ではKantara , OIX (OpenID Foundationが母体) が政府認定のTrust Framework Providerとして認定され、パイロットが実施されつつある
 - 他の欧米諸国にもその動きが波及しつつある。
 - * 詳しくは5/17日実施のOIDF-Jセミナー資料参照
 - * <http://www.openid.or.jp/modules/news/details.php?bid=52>

- 日本版Trust Frameworkの機運が高まり、OIDF-J内でWGが発足(2012/3~)

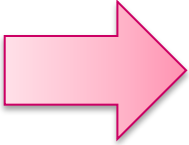
トラスフレームワーク (Open Identity Trust Framework) とは

オンラインで
アイデンティティ情報を
認定された事業者の間で
利用者本人の同意に基づき
流通させる信頼構築の枠組み



OIDF-J トラストフレームワークWG

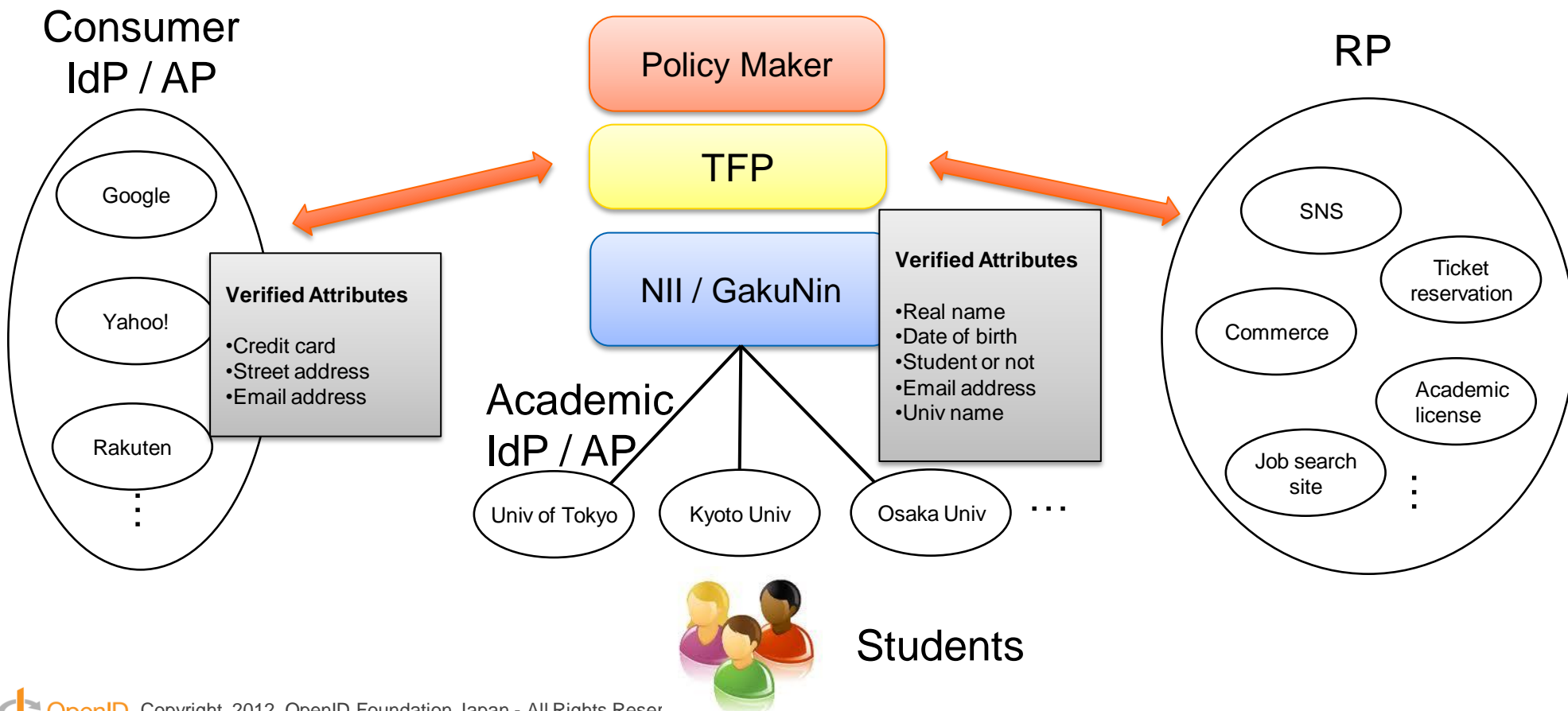
- 民間分野をつなぐアイデンティティ連携のためのトラストフレームワークの策定
 - 民間IdPと民間RP
 - 学術分野と民間ビジネス分野
- 信頼できるアイデンティティ・エコシステム実現のためのユースケースの策定と、トライアルサービスの実施
 - “Student Identity Trust Framework” (学認のもつ属性情報)
 - 確認済み(Verified)の属性情報の事業者間流通
 - 利用者の権利保護、ステークホルダー全員のメリット確保
 - 保証レベル2程度のIdPの認定



ユースケースを実際動かし、フィージビリティを行うことで、
トラストフレームワーク普及のためのブートストラップとし、
将来的に様々な分野・業界への横展開を狙う。

ユースケースの一例: Student Identity Trust Framework

- 学生はサイバー空間上でも同じようなベネフィット(学割など)を得ることができる
- IdPは外部から資格情報(学生という属性)を得ることで認証サービスの付加価値を上げることができる
- RPは学生の属性を得ることで、早期に顧客のログインができる。
- AP(各大学)はRPと個別に契約する必要がなく、NIIに代行してもらえる。学生に付加価値サービスを提供できる





GakuNin

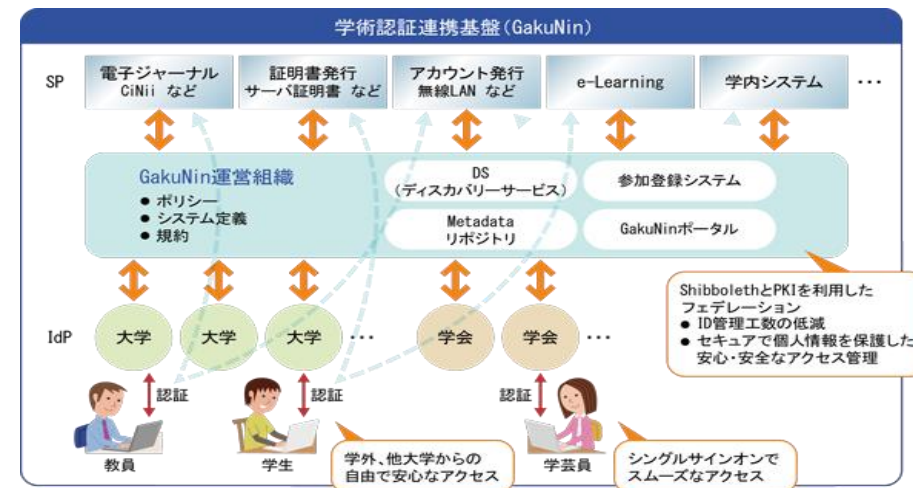
学認とは

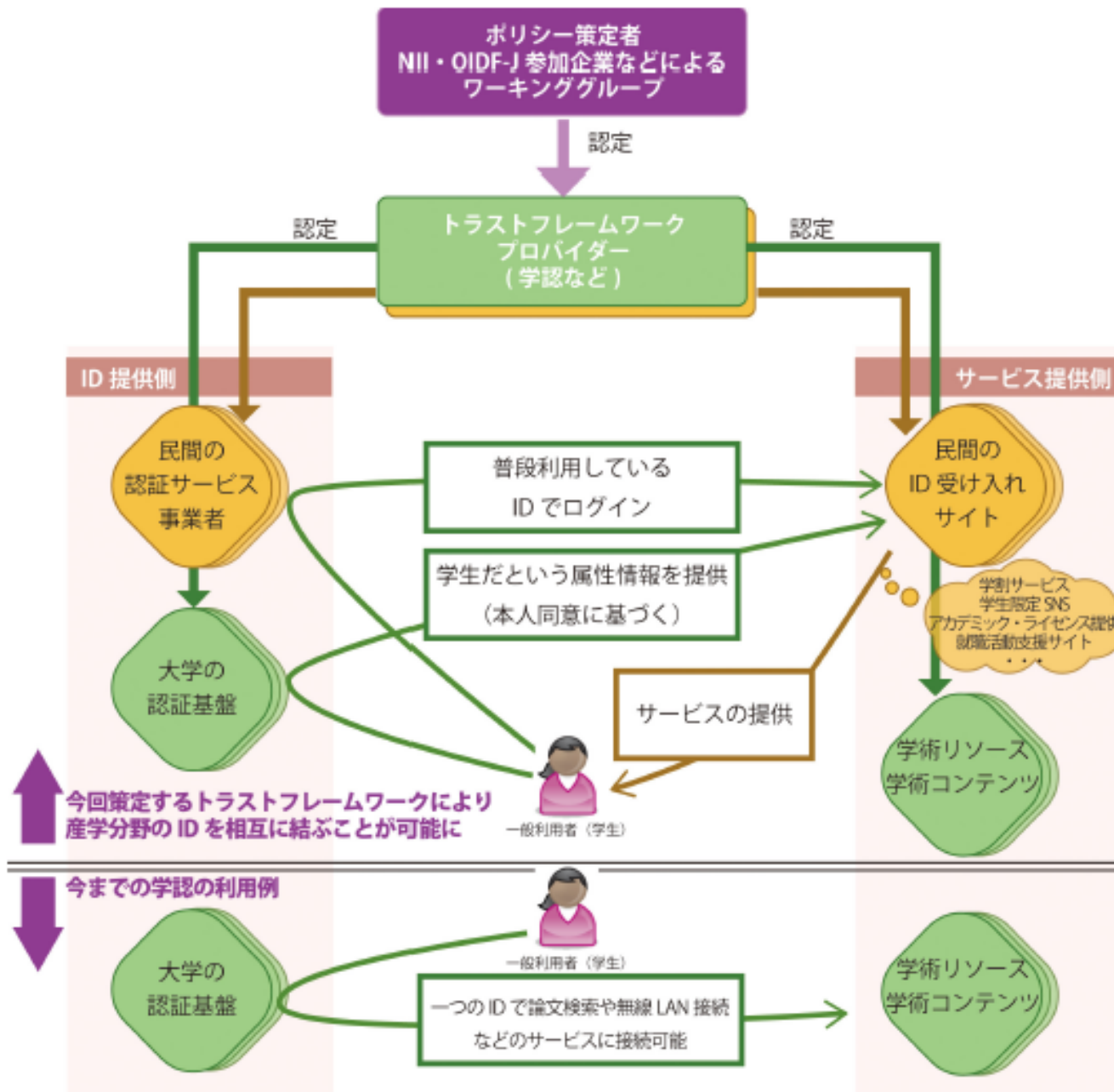
- ▶ **シングルサインオン(SSO)技術を用いて学術機関が連携**
 - ▶ **教育・研究のためのより良い(安心、安全、便利な)ICT基盤の構築を目指す**
- ▶ **学術機関が、その構成員であることと、属性情報について保証**
 - ▶ **サイトライセンスとの親和性が高い**

- ▶ **認証のための国際標準SAMLに準拠**
 - ▶ Shibboleth by Internet2
 - ▶ simpleSAMLphp by UNINETT

「学認」の役割

- ▶ **IdP / SP の運用基準(セキュリティレベル)統一**
- ▶ **やりとりする属性情報の統一(現在17種類)**
- ▶ **IdP / SP の勧誘、接続支援**
- ▶ **参加申請の受付**
- ▶ **メタデータ(IdP / SP リスト)の管理、配布**
- ▶ **DS (Discovery Service)の運用**
- ▶ **海外フェデレーション等との連携 など**





平成24年3月5日
国立情報学研究所
OpenIDファウンデーション・ジャパン
共同プレスリリース

「産学のIDをつなぐ世界初のトラストフ
レームワークの研究に着手
～利用者情報の安全な流通を目指し、
学生向けサービスの提供を支援～」

より

図：利用者の情報を産学間で安全に流通させるためのトラストフレームワークを策定

- TF-WGメンバ mixi伊藤さんのデモサイトを使ったSITF利用イメージ
 - <http://idcon.org/post/25642200247/sitf>

■ デモから見えてくること

- 属性情報の鮮度問題

- * 学生情報をキャッシュしていい・悪いはサービス内容によって決まりそう

- 学認-民間IDP間の紐付けは複数可能か？その場合

- * IdentityとAttributeが別々の箇所から提供される→IDPごとに仮名ID払出し含め要検討

■ Student Identity Trust Framework 構築に向けて

- (民間IDP)提供IDの保証レベル (LOA) 定義

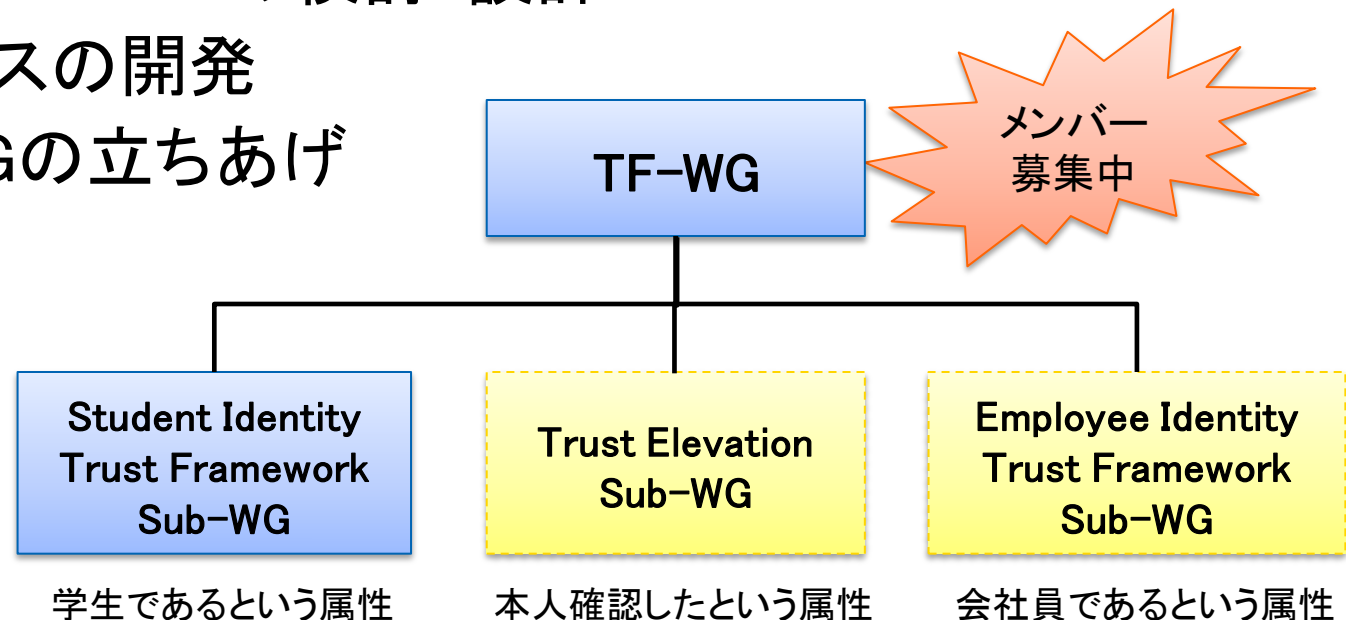
- (民間RP)提供される情報の利用ポリシー (LOP) 定義

- (学認)SITF利用サービスへのポリシー (LOAA) 定義

- パイロットサービスの本格的な立ち上げ

TF-WGのマイルストーン

- フェーズ1:2012/2-5
 - 学生IDを使ったユースケースの作成
 - IdP向けポリシー、RP向けポリシーの作成
- フェーズ2:2012/7-
 - SITFを使った実サービスの検討・設計
 - パイロットサービスの開発
 - 他分野のサブWGの立ちあげ



■ Employee Identity Trust Framework

- IdP(企業)とSaaS/Cloud/ASP事業者間のフェデレーション
- 会社提供の端末からBYODへ
- サムライクラウド利用者 だという資格情報をIdPからRPに提供し
リソースへアクセス

