



NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

カンターラ・イニシアティブ 分科会における取組み事例 ～SAML-OpenID連携～

NTT情報流通プラットフォーム研究所



NTT

「相互運用推進」取り組みのご紹介

カンターラ・イニシアティブの活動内容のひとつにアイデンティティ管理に関する相互運用性の推進がある。

ID管理技術間の相互接続が課題



Concordia Project にて一定の成果を得るなどしてきた



ID 管理技術の普及拡大にはより一層の協調が必要

<実際の取り組み事例>

・SAML-InfoCard連携: RSA Conference 2008発表

・SAML-OpenID連携: RSA Conference 2009発表【本日のご紹介】

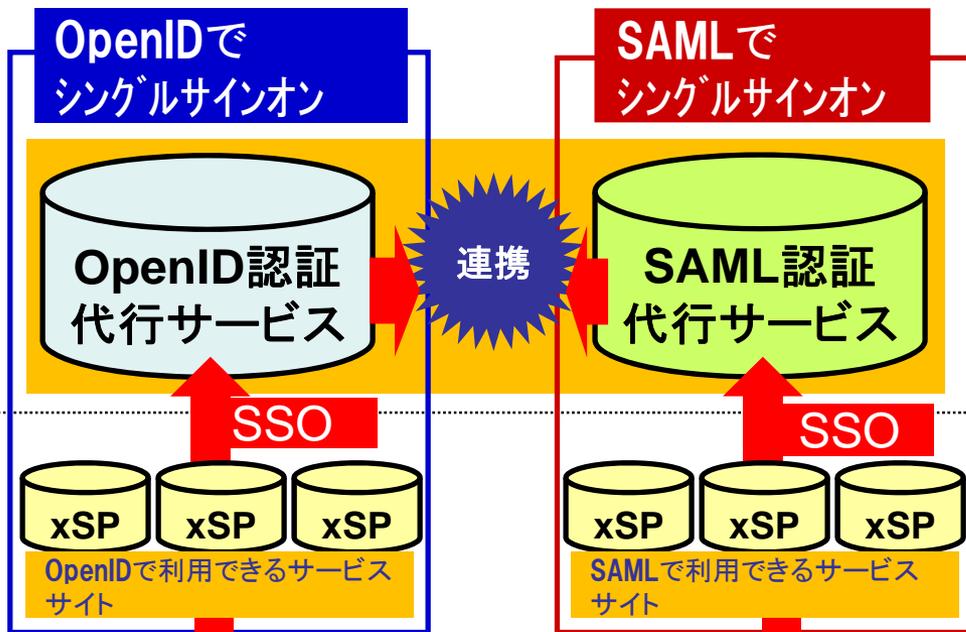
Oracle、NRI、NTT 3社による相互接続デモ

kantara
INITIATIVE

実現する“連携”

シングルサインオン方式 SAML・OpenIDの相互連携を実現

- SAMLサービスサイトの利用時に、OpenID認証サーバの認証結果を利用できます。
- OpenIDサービスサイトの利用時に、SAML認証サーバの認証結果を利用できます。



認証サーバ側メリット

SAML・OpenID 両サービス
とも接続可能 ⇒ 認証代行利
用サービスの増加

サービスサイト側メリット

SAML・OpenID 両認証サー
バとも接続可 ⇒ ユーザ増加

ユーザメリット

利用シーンにあわせたOpenID・SAML
アカウントの利用の使い分けを支援。



SAMLアカウントを持って
いるユーザでOpenID
サービスを利用したい人



OpenIDアカウントを持っ
ているユーザでSAML
サービスを利用したい人

デモをご覧ください

今回ご紹介するもの

- SAML仕様とOpenID仕様間での相互運用の実現をユースケースにあわせて示します。
- ユースケースは2つ
 - 1) OpenIDユーザがSAML-SPを利用できるシーン
 - 2) SAML-IDPユーザがOpenID-RPを利用できるシーン

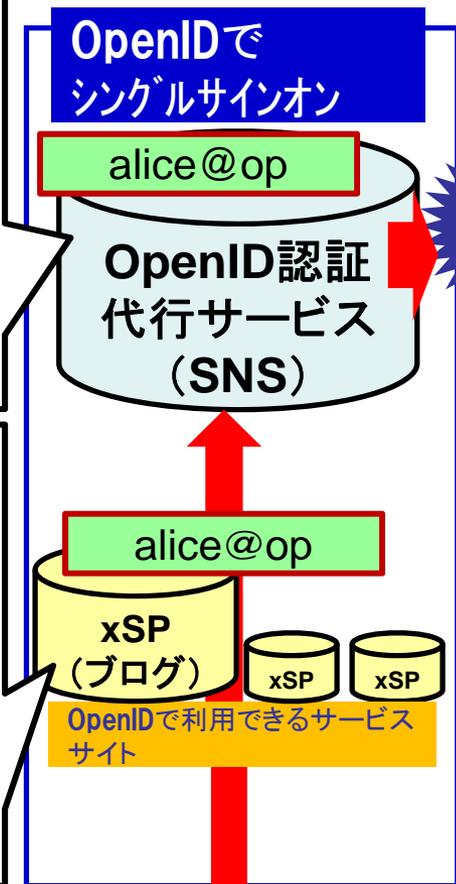


NTT

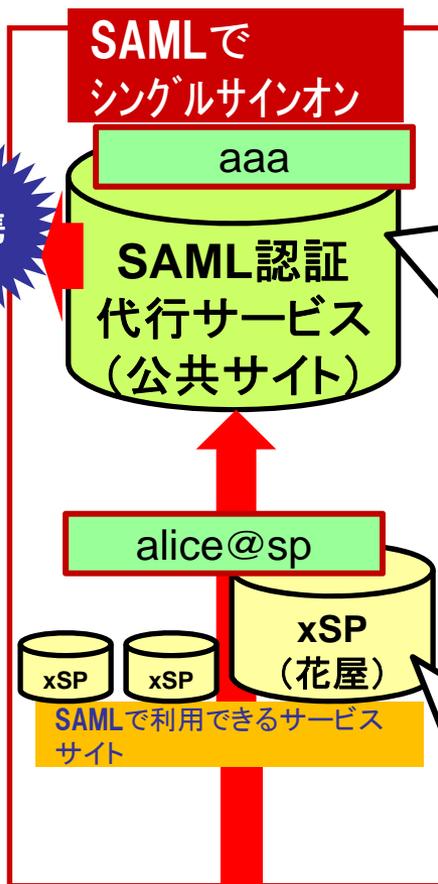
【デモ実施】デモシステムの前提条件

デモシステムにおける各サービスの前提条件は下記の通り

サイト種別	OpenID-OP
アカウント	あり (alice@op)
提供認証手段	ID・パスワードのみ



連携



サイト種別	SAML-IDP
アカウント	あり (aaa)
提供認証手段	①ID・パスワード ②PKI 認証

サイト種別	SAML-SP
アカウント	あり (alice@sp)
必要な認証	閲覧: ID、パスワード 購入: PKI 認証

すべてのアカウント連携済み



ユーザ: Alice

PKI証明書はインストール済み