NTTソフトウェア

【OpenID Tech Night vol.11】

TrustBind/Federation Manager紹介 OpenIDConnect編

2014年3月7日

NTTソフトウェア株式会社

Copyright© 2014 NTT Software Corporation. All rights reserved.

自己紹介

- 作田　宗臣　@spilamber
  - NTTソフトウェア(2010～)
  - TrustBind / Federation Managerの製品保守(OpenID/Oauth/OpenID Connect)担当
    - OAuth2.0機能とOpenID Connect機能はワシが育てた
  - OpenIDファウンデーションジャパンでは以下のWGに参加中
    - Enterprise Identity WG
      - OpenID Connect 技術タスクフォース
    - 翻訳・教育WG
      - JWTとOIDC Coreの翻訳の一部

Copyright© 2014 NTT Software Corporation. All rights reserved.

当社のフェデレーション技術への取り組み

■Liberty Allianceの標準化活動の一環として、NTTグループでは仕様準拠プロダクトの開発を行ってきました。
SAMLやID-WSFなど、同団体の技術仕様については、世界に先駆けての開発実績を有しております。

TrustBind® Federation Manager

LIBERTY ALLIANCE INTEROPERABLE IOP.PROJECTLIBERTY.ORG

- 2002年、NTT情報流通プラットフォーム研究所にて開発開始
- 2003年、世界最初のLiberty Alliance認定試験に合格
- 2004年、仕様更新に伴う新認定試験にも合格
- 2006年11月、SAML2.0に対応したパッケージソフトウェアとして、
  NTTソフトウェアより「TrustBind/Federation Manager」として販売開始
- 2006年12月、2008年9月の2回にわたりSAML2.0認定試験に合格
- 2008年、Version1.1にて、携帯用ゲートウェイであるMobileGateway Editionを販売開始
- 2009年、OpenID Authentication 2.0に対応したVersion1.2を販売開始
- 2010年、ID-WSF 2.0(SAML仕様に基づく属性交換)に対応したVersion1.3を販売開始
- 2010年、OpenIDの拡張仕様(属性交換)に対応したVersion1.4を販売開始
- 2011年、システム導入の手間を大幅に削減したVersion1.5を販売開始
- 2013年、OAuth2.0およびOpenID Connectに対応したVersion1.6を販売開始

※TrustBindはNTTソフトウェア株式会社の登録商標です。

Copyright© 2014 NTT Software Corporation. All rights reserved.

なぜ今OpenID Connectなのか

- エンタープライズ向けにOpenIDの代替プロトコルとして
  - 今後出てくるだろうモバイル向け対応
  - RP側の実装が容易
  - モジュラーデザインで、実装範囲の取捨選択が可能
  - OAuthプロトコルも使える
  - セキュリティをPKIベースできちんと担保できる

- NTTグループ内で最新仕様に追従していくのは、
  NTTソフトウェアの責務でしょ！？

Copyright© 2014 NTT Software Corporation. All rights reserved.

TrustBind® Federation Manager

クラウドセキュリティの不安、解消します。

ソリューション導入のメリット

クラウドサービスに対する認証連携・セキュリティ強化を実現

- 社内IDでログインした結果をクラウドサービスに引き継ぐことで、社外からの不正アクセスを防ぐことができます。
- 多要素認証により、クラウドサービス利用時の認証強化を実現することができます。
  - ✓ PKI/OTP/SMS/マトリクス認証に対応可能
    (*) 一部は他社製品との組合せにより実現

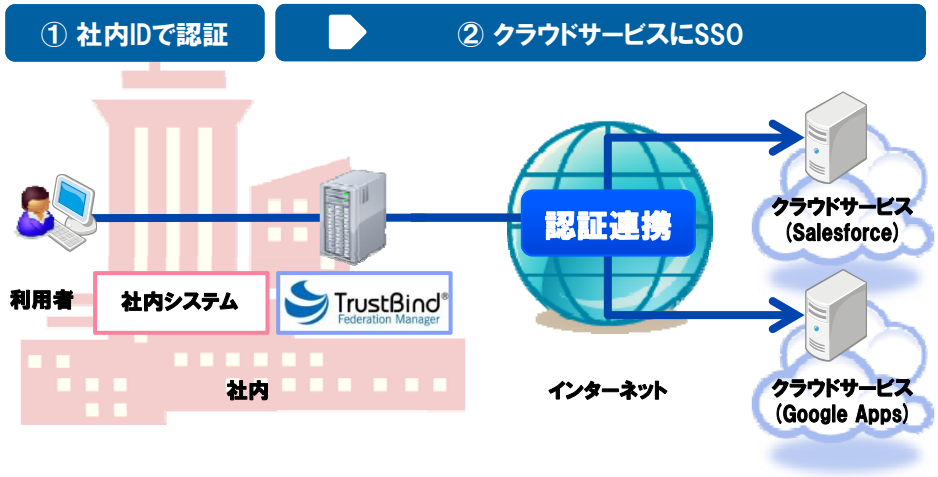
多様なシステムに対し低コスト・短期間で実現

- ご要望に合わせたシステム構成で、既存の社内システムとすぐに連携が可能です。また、カスタマイズ要件にも柔軟に対応できます。

多くの実績と信頼

- NTTグループ内のサービス基盤への導入を中心に、数多くの実績があります。
- 導入コンサルから保守までを トータルソリューション として手厚くサポートいたします。

社内システムで認証を行った利用者は、新たに認証操作を行うことなく、認証連携しているクラウドサービスにアクセスすることができます。



既存の社内システムを活用し
短期間に！簡単に！
安全・安心なクラウド利用をサポートします。

TrustBind/Federation Manager は
SAML2.0, OpenID, OAuth2.0, OpenID Connect
といった標準規格をサポートしています。

LIBERTY ALLIANCE INTEROPERABLE
IOP.PROJECTLIBERTY.ORG

Copyright© 2014 NTT Software Corporation. All rights reserved.

TrustBind/Federation Manager@OIDC

- OpenID Connect 仕様対応状況（2013/09現在）
  - OpenID Connect Messages 1.0 draft 16
    - http://openid.net/specs/openid-connect-messages-1_0-16.html
  - OpenID Connect Standard 1.0 draft 17
    - http://openid.net/specs/openid-connect-standard-1_0-17.html

- 主な特徴

1. 社内の既存認証画面をそのまま活用したい
   - 認証処理と認可処理を、既存の認証画面に置き換え可能

2. プロトコル中に追加で処理を行いたい
   - 処理中の各所（電文の受信直後や返却直前）で拡張が可能
   - UseinfoEndpointに関しては、返却する属性をカスタマイズ可能

3. 今使っているデータストアをそのまま使いたい
   - データストアのインタフェース化
   - 標準で, Oracle, PostgreSQL, MYSQLに対応

Copyright© 2014 NTT Software Corporation. All rights reserved.

今後の展開(予定)

- 管理者向けWebインタフェースの拡充
  - 運用機能の拡張
  - OAuth機能で実装済みのClient管理インタフェース@OIDC版
- エンタープライズ向けの拡張
  - EI-WG向け拡張
  - SCIMの実装も合わせて実施
- プロトコル関連での展開
  - Core以外のProfileに対応
  - OpenIDとのセッション共有等、マルチプロトコルを実現

Copyright© 2014 NTT Software Corporation. All rights reserved.

まとめ

- どうしてOpenIDConnect？
  - OpenIDではできないことができるプロトコルとして
  - NTTグループ内ではNTTソフトがやるべきこと

- TrustBind@OIDC
  - OpenID Connectのプロトコルはそのままに、
    カスタマイズ性に優れる
  - 今後は、プロトコル拡充はもちろん、使いやすさも追い求める

NTTソフトウェアは、今後とも
OpenIDファウンデーション・ジャパンと連携しながら、
ID・認証連携の普及に努めていきます！

Copyright© 2014 NTT Software Corporation. All rights reserved.