カンターラ・イニシアティブ・シンポジウム 2009 ～ 事例研究 ～

ORACLE®

事例でみるID管理技術の使い分け~~(仮)~~

日本オラクル株式会社 Fusion Middleware事業統括本部
Security SC部
澤井真二, CISSP

はじめに

- この資料の目的
  - 事例や実績を引用しながら、ID管理（アイデンティティ管理）に係わる技術を考えてみること

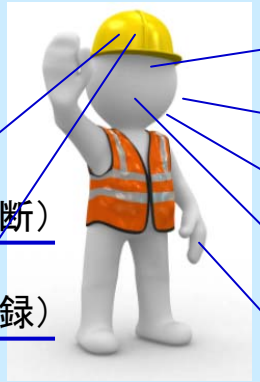
> 今回の事例や実績は、弊社（Oracle）の視点で書いています。

- 内容
  - 仮想世界 と IDの役割
  - SAMLを使用したフェデレーション利用の実績
  - 整理
  - 追加事例（XACML等）
  - まとめ

仮想世界とIDの役割

- IDとは？
  - システム利用者を識別するための情報。
  - システム利用者の役割を表現するための情報。

現実世界における存在確認の方法



脳（判断）

脳（記録）

目（表情・骨格・服装）

耳（声を聞く、足音）

口（声をかける）

鼻（匂い）

手（触れる）

個人を特定する情報：
・氏名、住所、誕生日、性別、家系、国籍 等

証明書

権利（免許証、社員証）

仮想世界における存在確認の方法

1．取得可能な情報

個人が保持する情報

・ログインID
・パスワード
・ICカードのID
・生体情報（指紋等）
・・・

アクセスポイントの情報

・IPアドレス
・ドメイン
・個体の番号
（MACアドレス等）
・・・

2．判断方法（処理）

・**認証**
※ 個人の特定

・**認可**
※ 判断と制御

・**証跡（ログ）**
※ 記録

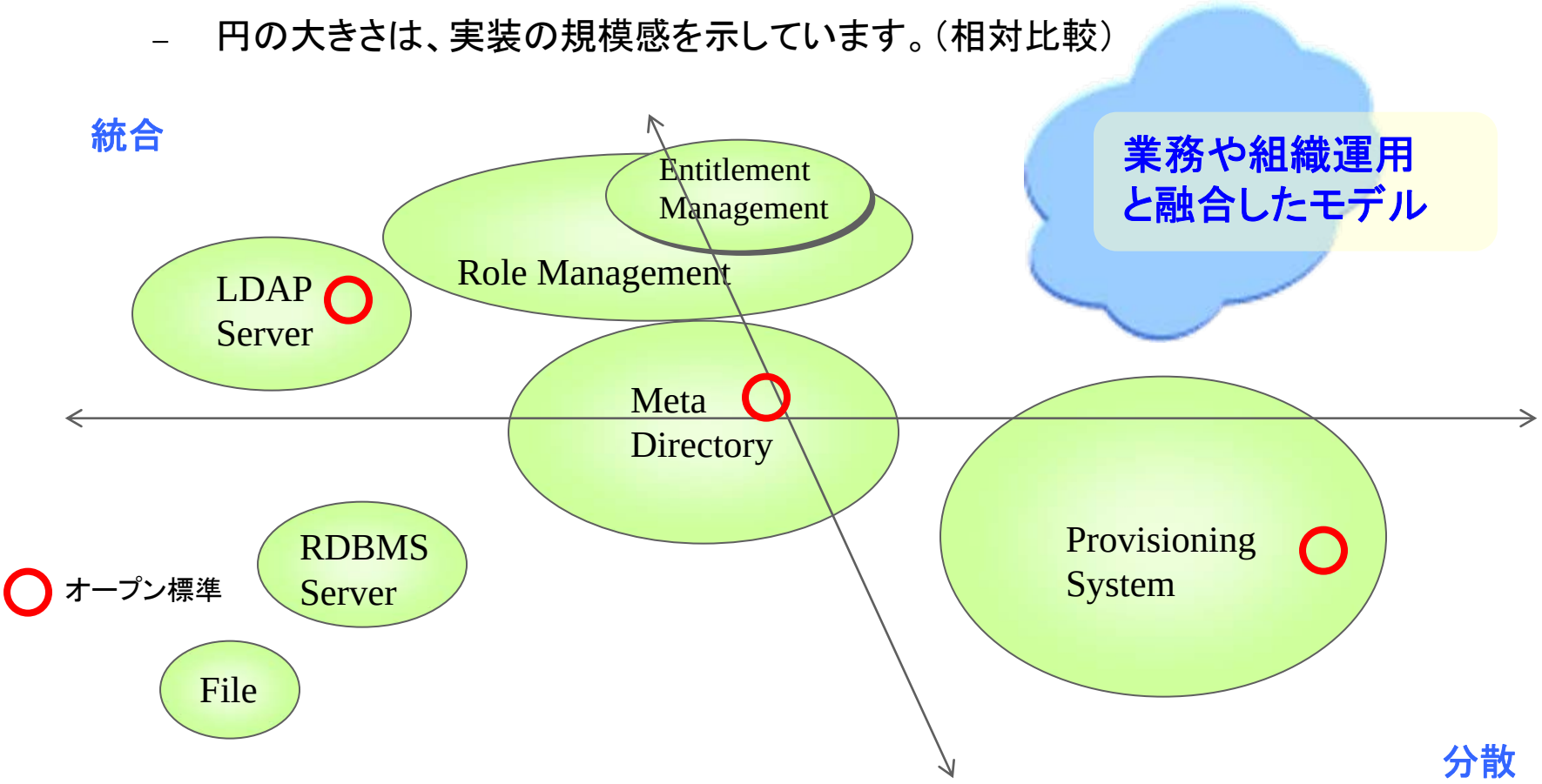
SAMLを使用したフェデレーション利用の実績 by Oracle

- 過去の実例より、ID管理に関連する次のケースを参考にして考えてみます。

	業種	課題	対策	利用技術
国内 A社 ＜部門間＞	製造	特定の拠点（地域）の社員を、 別事業部が管轄する ERP を利用させたい。	2つの拠点のローカル認証 システム同士を連携する。	SAML 1.1 アサーションによる 認証状態の連携（SSO）。
		フェーズ　ローカルの認証機能 → SAMLによる連携		
海外 B社 ＜企業間＞	運輸	ITコスト削減、利用者増や業務パートナーとの共有基盤の推進、パスワード数削減。	情報系システムの 統合認証基盤を構築する。	LDAPによるID情報の集約化。Web SSOシステムとICカード認証（多要素認証）。SAMLによる認証状態の連携 。
		フェーズ　ID情報の集約化（LDAPデータの仮想統合） → 統合認証（SSO） → SAMLによる連携		
海外 C社 ＜企業間＞	金融	金融サービスをアウトソース（外部委託）し、異なるドメイン間で SSO を実現する。	標準技術による SSO化。	SAML 2.0 による認証状態の連携。 不正アクセスへの対策。
		フェーズ　ID情報の集約化（LDAP） 統合認証（SSO） → SAMLによる連携 → 不正アクセス対策（なりすまし対策）		
海外 D社 ＜企業間＞	製造	従業員、販売パートナー、関連子会社と連携するためのID基盤が存在しない。	段階的にID管理技術を導入して、業務効率を改善する。人手に頼らない基盤作り。	ID管理、統合認証、フェデレーションを段階的に導入して、網羅的な統合認証基盤を整備した。
		フェーズ　統合ID（プロビジョニング） → 統合認証（SSO） → SAMLによる連携		

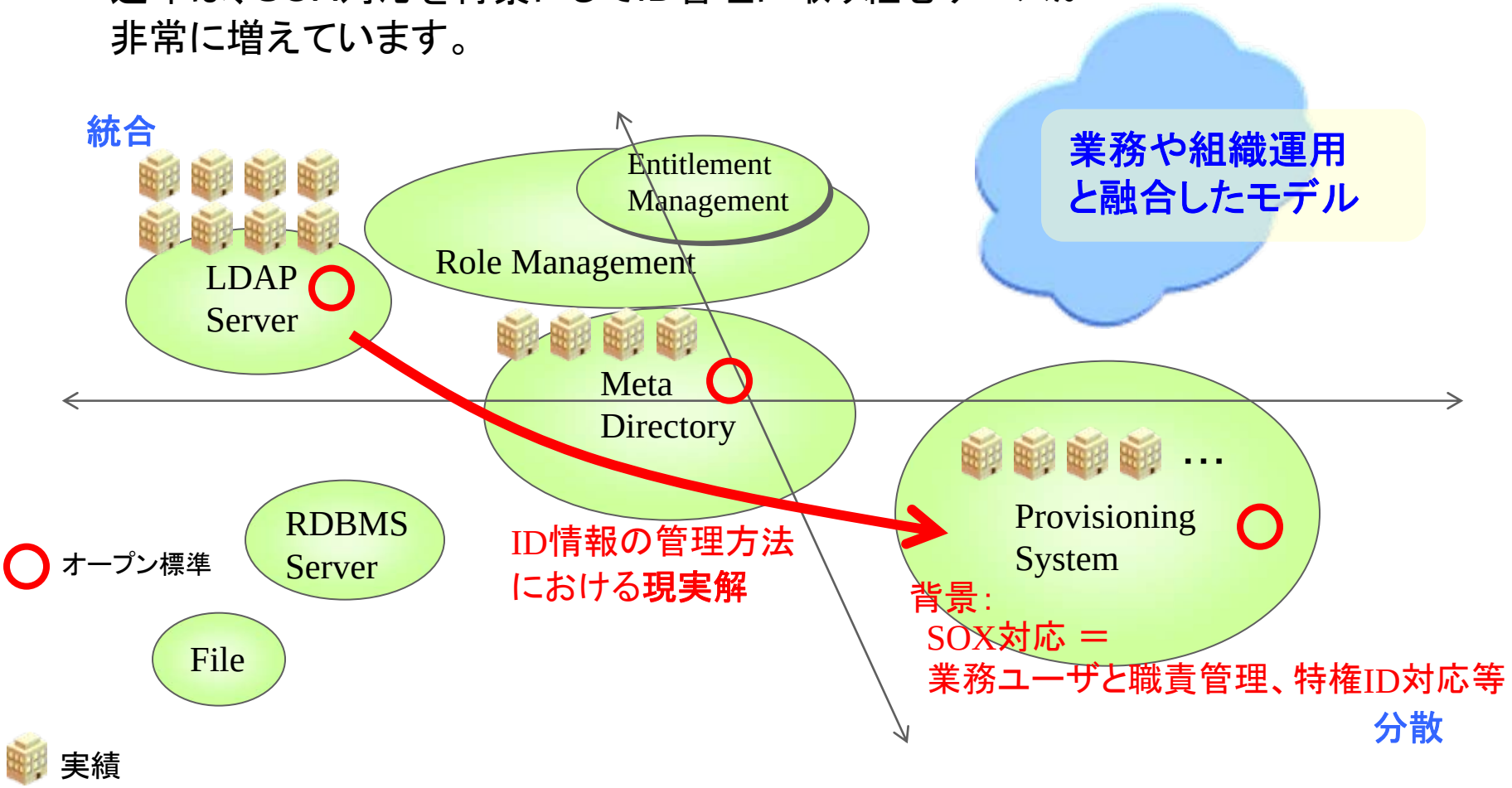
ID管理（ID情報の保管／ライフサイクル管理）- MAP

- この図では、ID管理の実装方式の傾向を示しています。
  - 右上の領域（雲の形）がゴールを示しています。
  - 円の大きさは、実装の規模感を示しています。（相対比較）



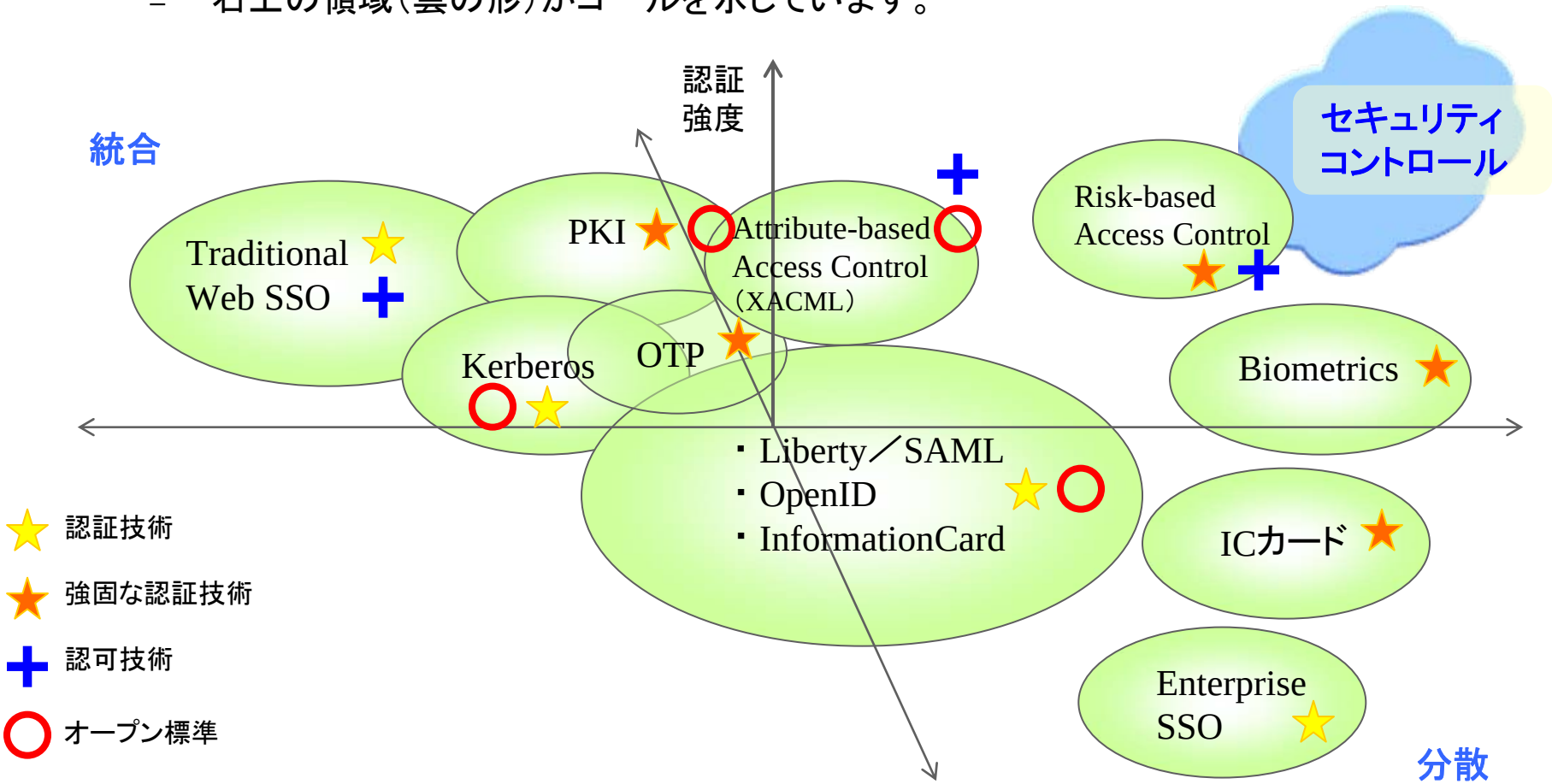
ID管理（ID情報の保管／ライフサイクル管理）- 実績

- この図では、ID管理の利用実績の情報を追加しています。
- 近年は、SOX対応を背景にしてID管理に取り組むケースが非常に増えています。



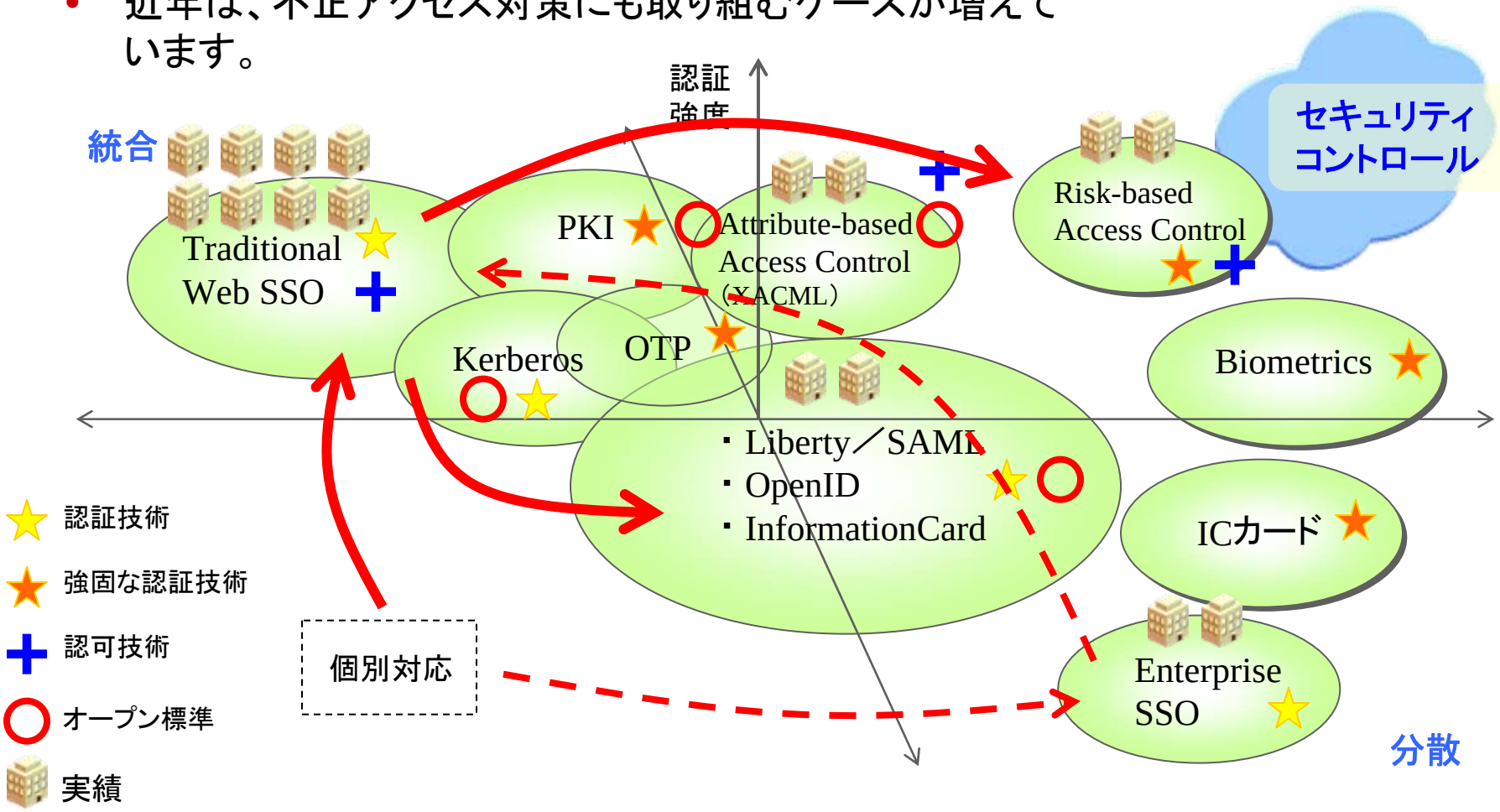
認証技術（ID情報による識別と許可）- MAP

- この図では、認証技術（認可含む）の実装方式の傾向を示しています。
  - 右上の領域（雲の形）がゴールを示しています。



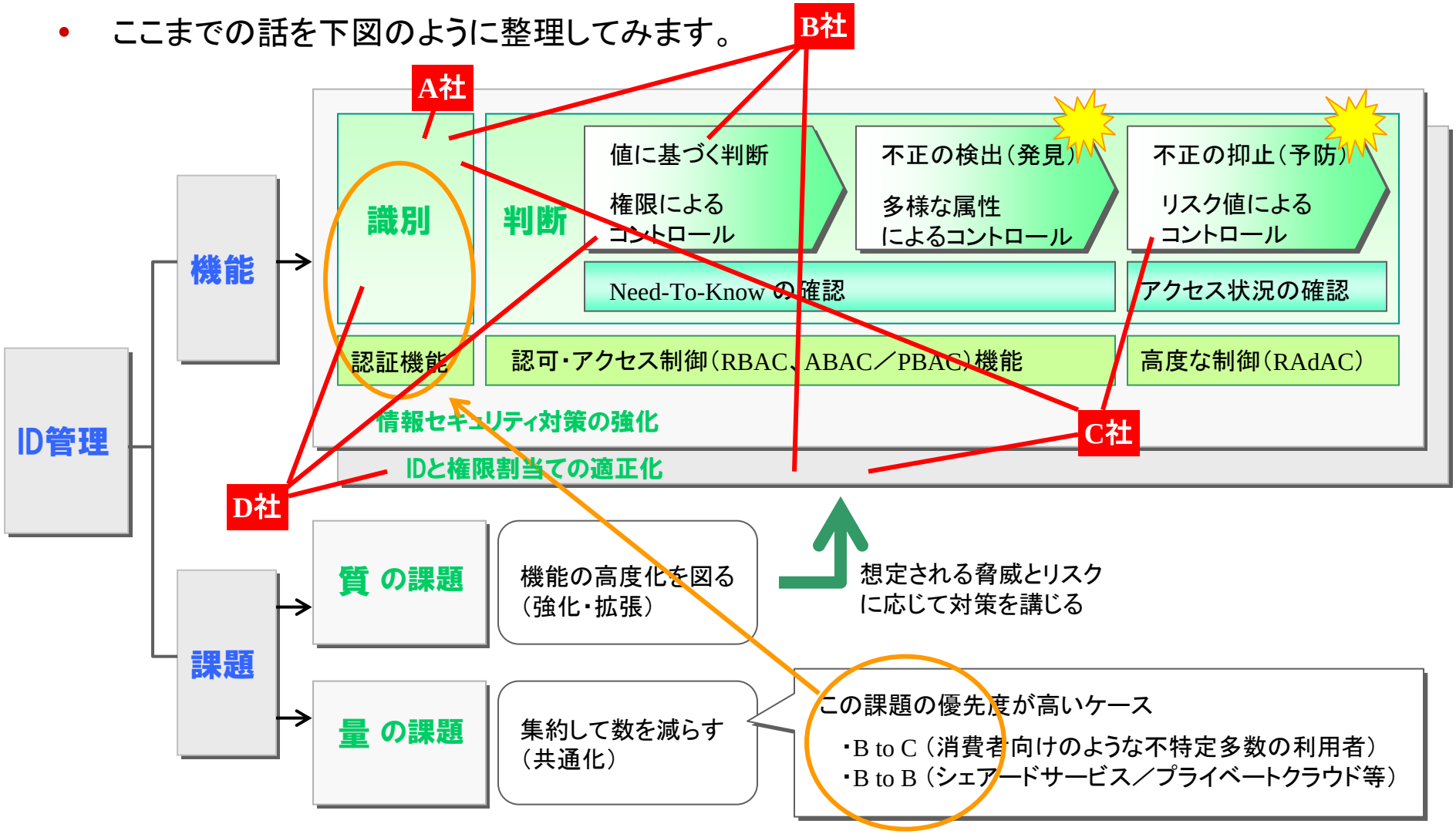
認証技術（ID情報による識別と許可）- 実績

- この図では、認証技術（認可含む）の利用実績の情報を追加しています。
- 近年は、不正アクセス対策にも取り組むケースが増えて
  います。



ここまでの整理

- ここまでの話を下図のように整理してみます。

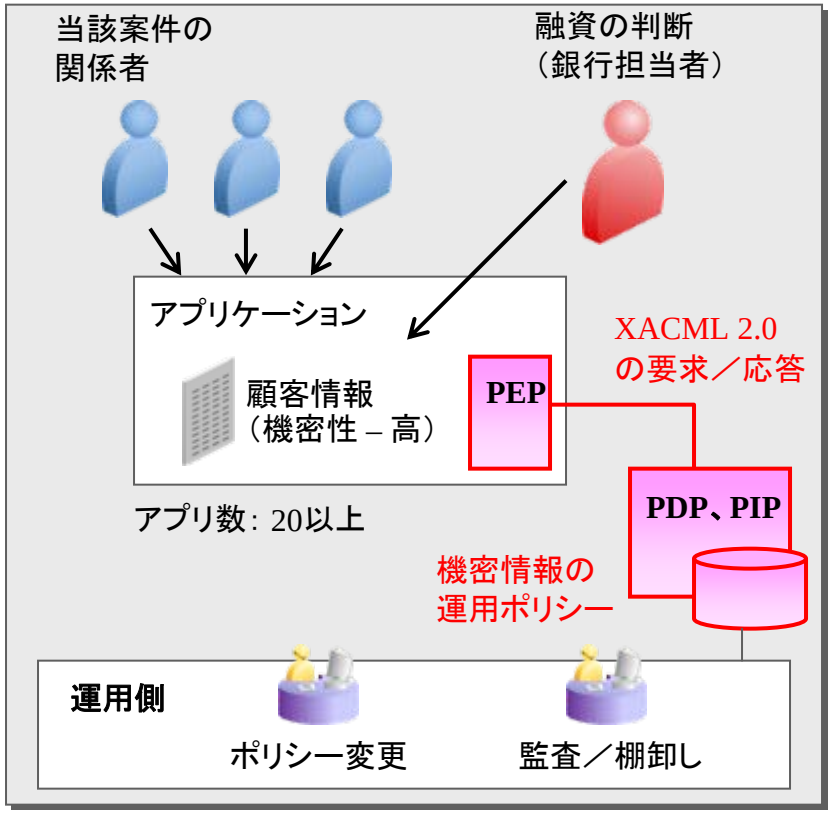


※ 参考情報：アクセス制御の方式（RBAC、ABAC、PBAC、RAdAC）について
http://csrc.nist.gov/news_events/privilege-management-workshop/

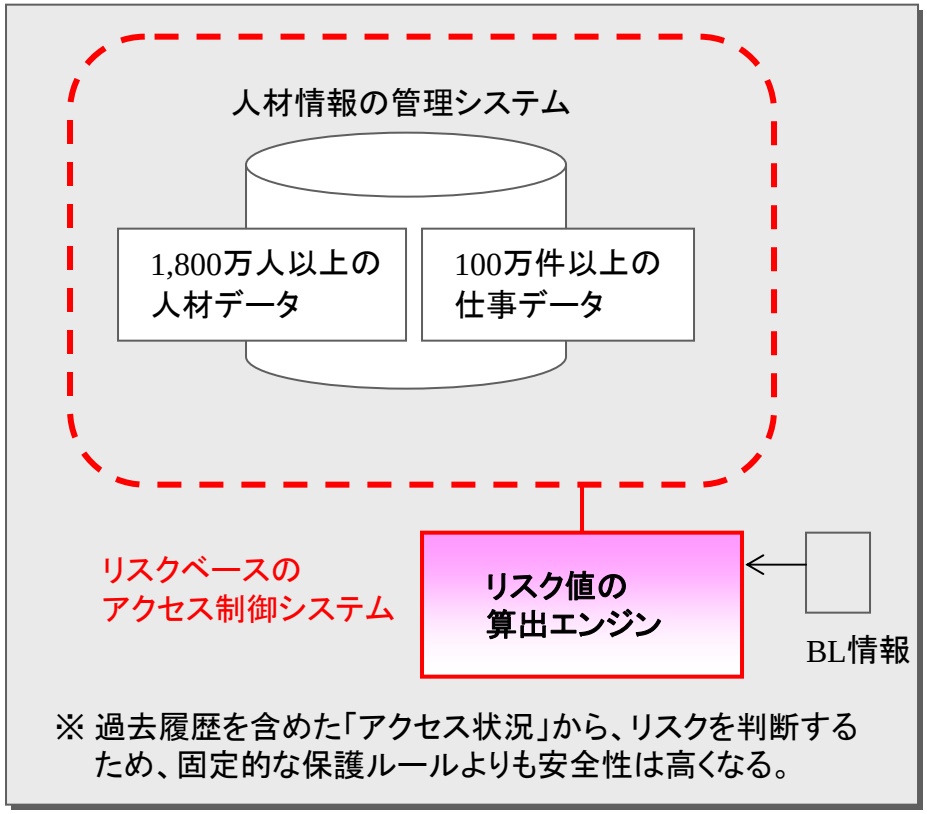
追加事例（1）XACML とリスク値に基づくアクセス制御

- システムの適正なコントロールのためには、**情報の精度** と **利用状態（サービスレベル）**を確保・維持することが重要と考えています。
  - 適切な**アーキテクチャ（テクノロジー）**を選択する
  - 適切な**アプローチ**を実施する

例1．金融機関（海外）のXACMLによるアクセス制御



例2．人材情報を扱う会社（海外）のリスクベースのアクセス制御



追加事例（2）IGFによるID情報アクセスのコントロール

- 実用例ではありませんが、2008年11月に OpenLiberty の活動の一環で Oracle Virtual Directory（LDAPゲートウェイ・ソフトウェア）と ArisID API を組み合わせた検証ケースが紹介されています。
  - ArisID API は、IGF（Identity Governance Framework）仕様を実装したOSS。CARML メッセージにより、ID情報を取得する機能を提供しています。

OVD Provider for ArisID - Developer Preview

18 December 2008

ArisID is an open source API designed for developers to access identity information using a single API that enables
identity information stored in different types of repositories accessed using different protocols. The API the first to im
Framework specifications from Liberty Alliance and in particular, uses **Client Attributes Markup Language** is a key
developers to create their own virtual identity database while retaining the ability to interconnect with enterprise ident

ArisID uses a declarative, multi-function API that depends on **providers** to do the work of data mapping, protocol tra
OVD Provider for ArisID is an example of one such ArisID provider. The OVD Provider for ArisID is a library that enat
services to an application using the ArisID API. Thus Oracle OVD plus the OVD Provider library for ArisID and the Aris
complete set of libraries that can be used by applications to access identity services.

ArisID is hosted by www.openLiberty.org. The API is available for use under the Apache 2.0 License. Oracle is a ma
information on ArisID, consult the wiki.

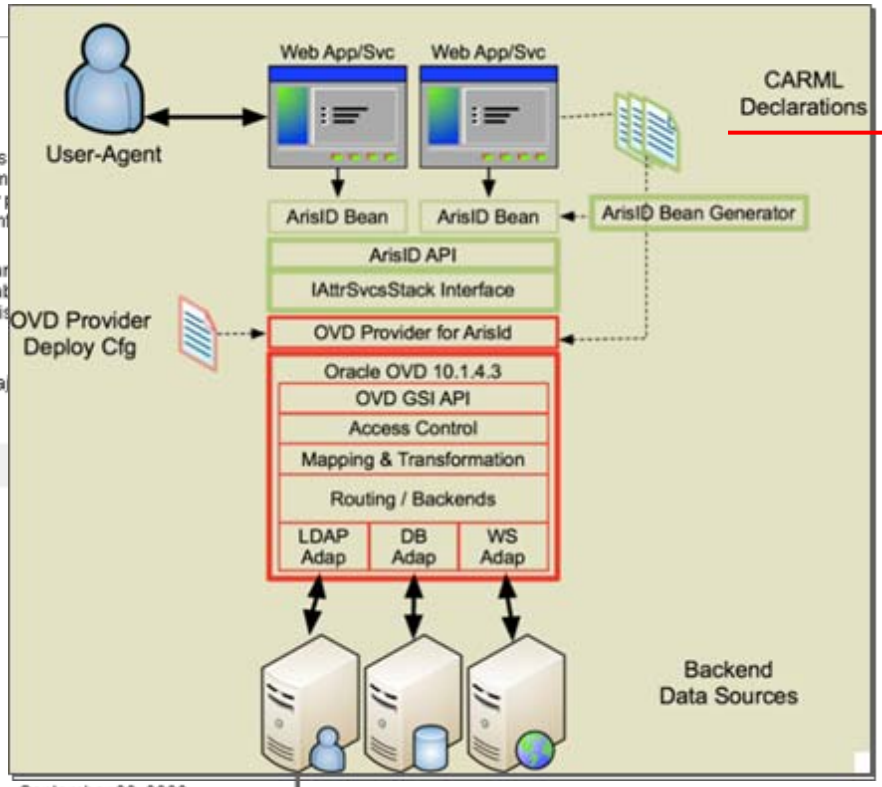
Description

ArisID Related Downloads

- OVD Provider for ArisID
- Oracle Virtual Directory 10.1.4.3
- OpenLiberty - ArisID Library

Resources

- Tutorial - Using OVD Provider for ArisID
- OpenLiberty ArisID Wiki
- Liberty Alliance IGF Specifications
- Oracle IGF Site



http://www.oracle.com/technology/tech/standards/idm/igf/arisid/index.html

Oracle は何故、認証・認可（アクセス制御）を気にするのか？
～ OpenID や SAML を利用する事例が少ない？ ～

- Oracle にとっては、ID は「システムの利用者」「組織に所属する人を示す識別子」として扱っており、情報セキュリティと効率化対策がID管理への取り組みのメイン。
- ID管理をパブリックなプロバイダに委託することは、前提条件ではない。

ORACLE

ERP（HR）

・ID情報の源泉
・業務ユーザの統制

情報系アプリ

・利用者の識別（個人認証）
・利用者のアクセス制限（認可）

RDBMS（データ）

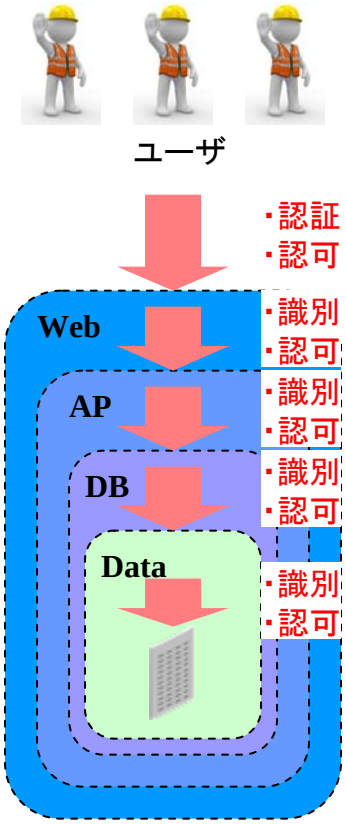
・価値の高いデータの保護

ERP
ERP
ERP

情報系アプリ
情報系アプリ
情報系アプリ

業務フロー（ワークフロー）の整備

・オープン標準のI/Fによる連携
（**SAML**による認証状態の連携を含む）

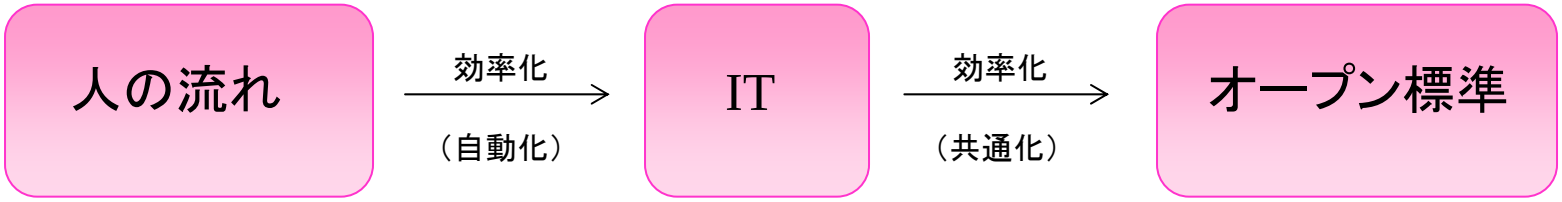


ORACLE

まとめ

- 今回、次のことをお伝えしました。
  - ID管理技術といっても、普遍のプロセスは存在しない。
    - 事例をもとにご紹介しました
  - ID管理とは、仮想世界で人をコントロールするための技術。
    - 識別して、管理して、不正を抑止するための方法
  - IDの信頼度は、情報の精度、認証レベル（認証強度）、セキュリティレベルに依存する。

IDに関して...



参考情報1. 統合認証基盤のためのソフトウェア
～ Oracle セキュリティ・プラットフォーム ～

- 企業の情報セキュリティ対策を支援するためのソフトウェアおよび機能を提供しており、世界中で多くの実績を持っています。

1. 統合認証基盤の基本機能（Oracle Identity and Access Management Suite）

アイデンティティ（ID）管理	
LDAP	**IDライフサイクル管理**
Oracle Internet Directory Oracle Virtual Directory	Oracle Identity Manager

認証・アクセス制御（アクセス管理）	
統合型認証・アクセス制御	**連携型認証（フェデレーション）**
Oracle Access Manager	Oracle Identity Federation

2. 補完機能

ロール管理
Oracle Role Manager

シングル・サインオンの強化
Oracle Enterprise Single Sign-On Suite

Webサービス・セキュリティ
Oracle Web Services Manager

認証・アクセス制御の強化
Oracle Adaptive Access Manager Oracle Entitlements Server

データ・セキュリティの強化
Oracle Advanced Security Oracle Database Vault Oracle Label Security Oracle Audit Vault

電子文書の取扱いに関するセキュリティの強化
Oracle Information Rights Management

http://www.oracle.com/lang/jp/products/middleware/identity-management/identity-management.html

参考情報2．おでんの具材

- 鍋に何を入れますか？

・大根

・こんにゃく

・練りもの

・たまご

・牛すじ

・ウインナー