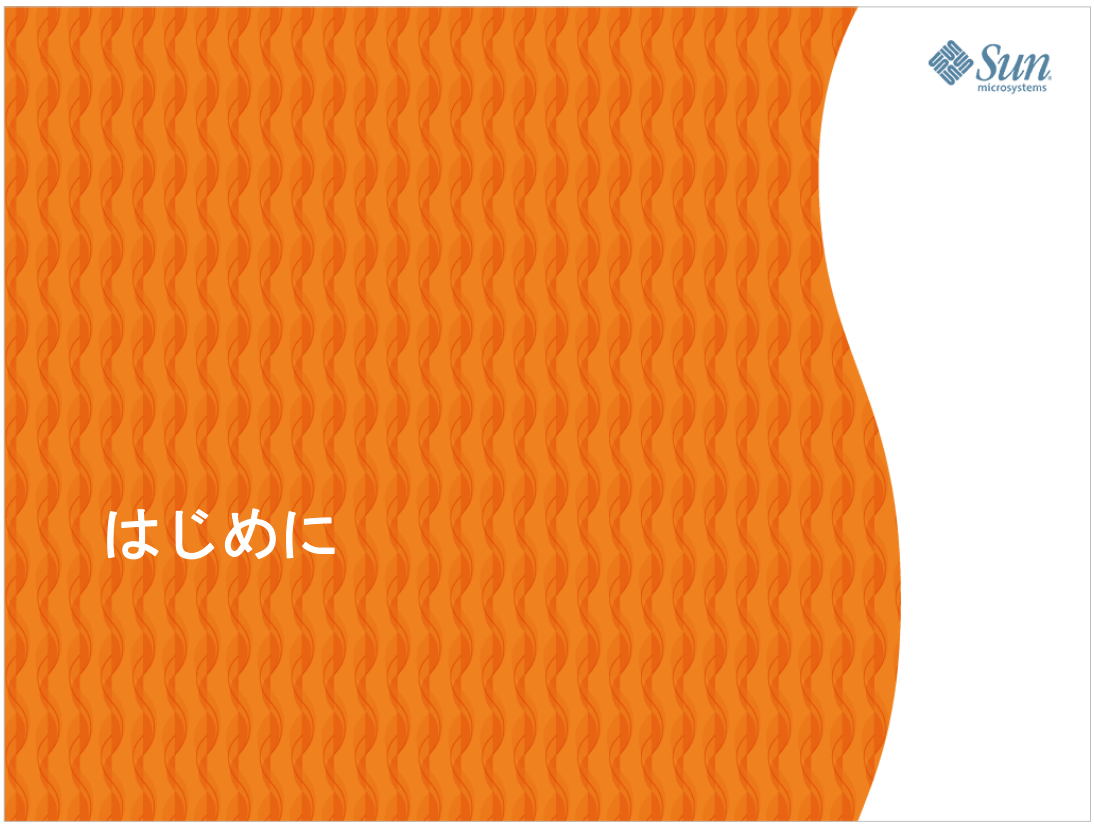


セキュアな Web サービスの時代

- セキュリティって暗号化のことではありません！！
  - > 昔：セキュリティ専門家 = 数学者
    - >暗号化技術そのもの
- HTTPS で OK?
  - > No,No! それってポイント to ポイントセキュリティ
  - > Web サービス（言葉が適切か否かは別として）時代にはエンド to エンドのセキュリティが重要
  - > メッセージそのものが”セキュア”である必要があります！

今、注目される SAML / Liberty

- まずはシングル・サインオン
  - > ユーザが最も利便性を感じる時（のうちの一つ）
  - > 様々な思惑と政治のプレッシャーの下、世界最高レベルのソフトウエア技術者が策定した、サービス時代の XML ベースの技術仕様
- SSO はユーザの目的ではない！
  - > 何のために SSO がいるか？
  - > 信頼のできるサイトからサービスを安全に使うことがユーザの目的
  - > Liberty はアイデンティティ Web サービスのための仕様！

SAML 登場の背景

- 様々な e-commerce 標準が開発
  - > Business transactions (e.g., ebXML)
  - > Software interactions (e.g., SOAP)
- その一方でセキュリティ分野は十分に標準化されていなかった
  - > PMI（Privilege Management Infrastructure ）ソリューション間の相互互換性の低さ
  - > Tight coupling within components コンポーネント内部での実装依存
- その一方で Web ベースの様々なコマースが考案されつつあった：例：federation

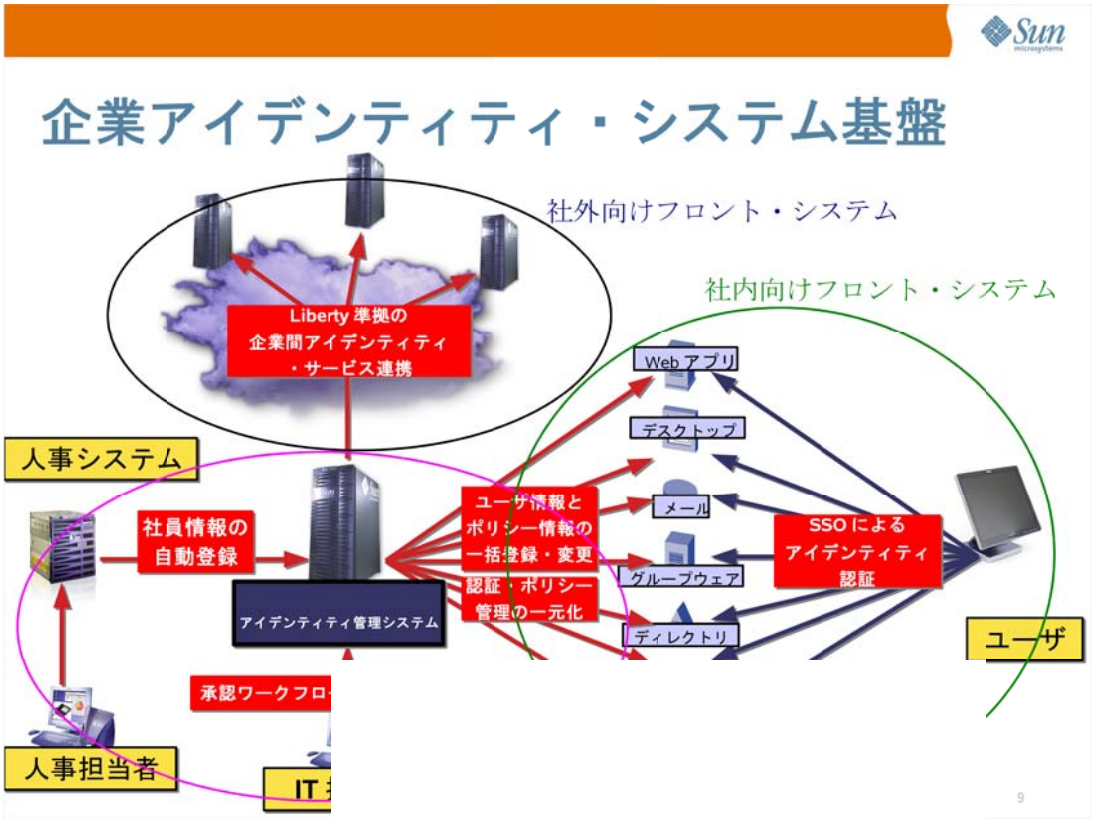
SAML / Liberty

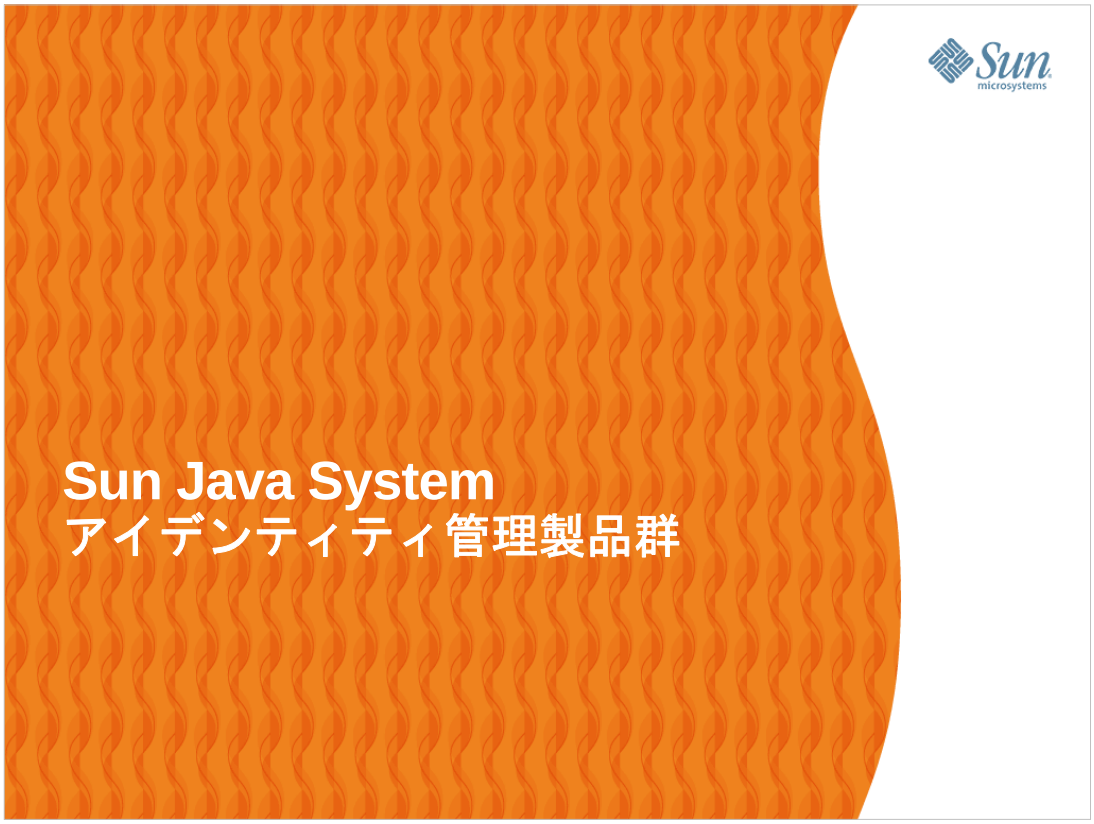
- これからのセキュアな Web インフラに必須の技術
  - > 仕様固めは終了
  - > ほとんどのベンダーがサポート
- エンド to エンドのセキュリティを確保するサービスインフラが必須
  - > SAML アサーションのような考え方が PKI に取って代わる？
  - > XML による汎用性はすべてのデバイスで共通に使われる
- Java プラットフォーム上への実装が進む
  - > Web コンテナベースの製品
  - > Java ディベロッパなら今すぐ始められる！

アイデンティティ・システムへの技術的アプローチ

- 「使う」技術
  - シングル・サインオン（ Signle SignOn)
    - 利便性の向上
    - 個人に対する利益の還元
  - サービス連携技術
    - 利便性のさらなる向上
    - 新サービスの提供
- 「管理」技術
  - アクセス・コントロール
    - データに対する利用制限
  - データ同期
    - 一貫性の提供
  - プロビジョニング
    - 自動化による集中管理・フロー制御

アイデンティティ管理を構成する技術的要素





Sun アイデンティティ管理製品群

包括的なソリューション

- オープンで統合可能なため、どんな環境にも適用可能
- 異機種環境でシステムへのセキュアなアクセスが可能
- 既存 / 新規のビジネスモデルに対し、迅速に対応
- セキュリティを強化し法規制等コンプライアンスに適合
- ビジネスプロセスを合理化と同時にセキュアなものとする

Sun Java System Directory Server Enterprise Edition

企業内導入からサービス・プロバイダまで幅広い用途に対応するための高い；

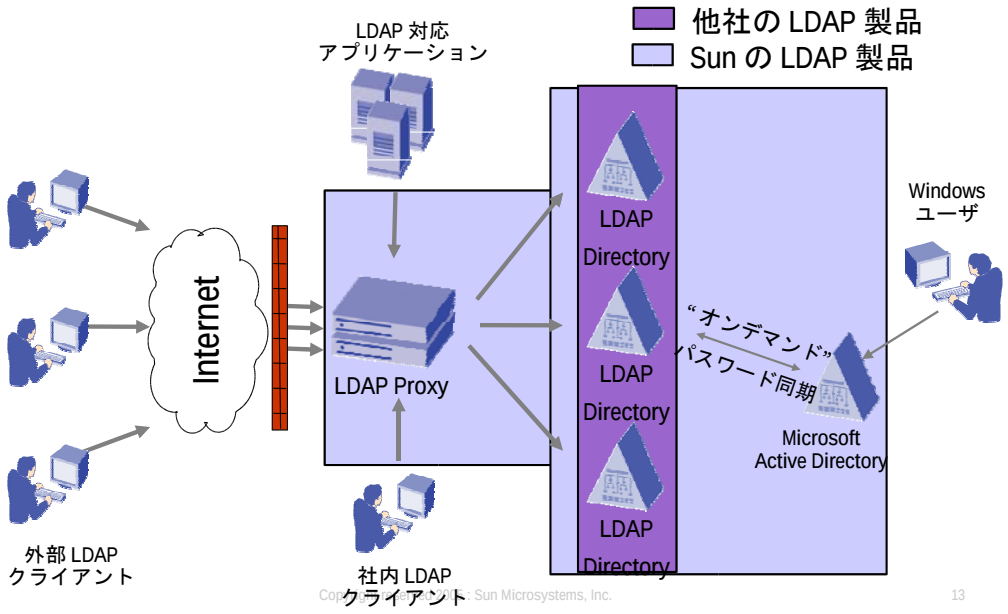
- 処理性能
- 拡張性
- 信頼性
- 可用性
- 管理性

を実現する“業界標準”LDAP ディレクトリ・サーバ

主な特長

- 全世界で 15 億ライセンスの販売実績
- LDAP v3 の実質的な参照実装
- 64-bit キャッシングと 12CPU に及ぶリニアなスケーラビリティ
- 4-way MMR (マルチマスタ・レプリケーション) および WAN 環境 MMR による可用性
- ロールおよびサービス・クラスによる ID 情報の効率的な管理
- LDAP Proxy 機能
  - 負荷分散
  - フェイル・オーバー
  - DoS 攻撃の防止
  - LDAP レスポンス・フィルタ機能
- Microsoft Active Directory との双方向同期機能

Sun Java System Directory Server EE
完全な企業ディレクトリの構築



Sun Java System
Access Manager

SAML や Liberty Alliance 仕様による連携サービスをサポートする、セキュアかつスケーラブルなアクセス管理プラットフォーム

- セキュリティの改善
- ビジネス機会の創出
- Web/Application の統合による効率化
- ユーザの利便性と生産性の向上

LIBERTY ALLIANCE INTEROPERABLE

“... アイデンティティ連携の仕様である Liberty および Security Assertion Markup Language (SAML) の実装において業界をリード”
August 2003 -- Burton Group

主な特長

- 認証処理の集中化
- ロール及びルールベースの認証
- 最新の SAML 1.1 / Liberty v2 サポートによる外部 ID 管理システムとの連携サービス
- Windows デスクトップ環境を含むシングル・サインオン
- 多様な API / プラグイン API による機能拡張
- 大規模サービス・プロバイダー用途にも耐えうる実証された拡張性

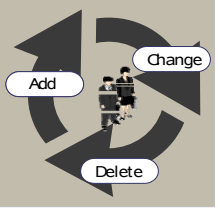
Sun Java System Identity Manager

業界初ユーザ情報のプロビジョニング・同期を提供する ID ライフサイクル管理ソリューション

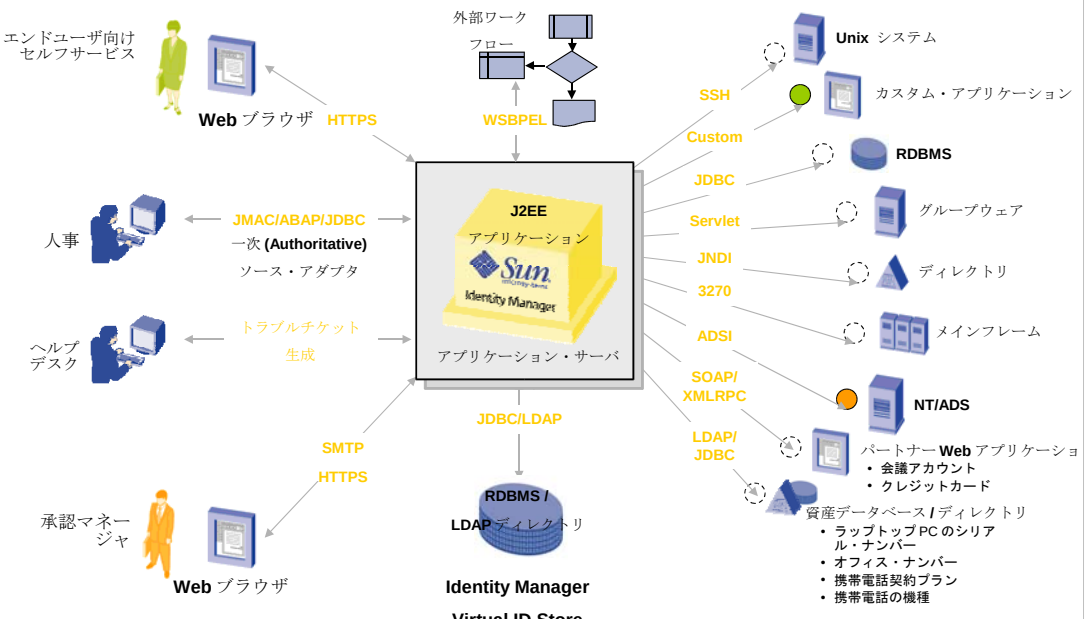
- 散在する ID 管理リソースを統合
- 複雑性と運用コストの低減
- セキュリティ・レベルの改善
- 様々な法的規制に準拠することを可能に
- サービスレベルの向上
- ビジネスプロセスの改善

主な特長

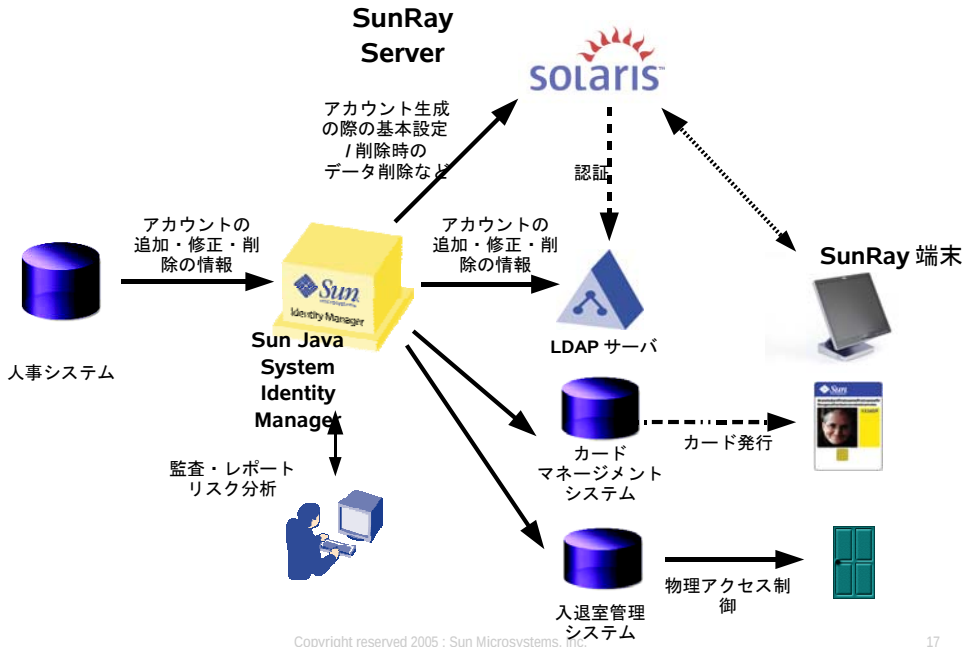
- 企業内の全ての ID 情報を一元的に表示・管理
- 複数の情報リソースに格納されているID情報の変更を自動的に検知
- 変更された情報をポリシーに基づき各リソースに伝播
- 管理権限の委譲
- セルフサービス機能により、ユーザ自身によるパスワード管理、権限変更申請
- 情報の変更通知や許可申請を自動的に行うダイナミック・ワークフロー機能
- 監査・レポート機能



Identity Manager: アーキテクチャ



SunRay+Solaris+Identity Managemet System



17

Sun Java System Access Manager 概要

Access Manager の位置づけ


OpenSSO


Access Manage


Federation Manager

Developer

- 認証
- Single-domain SSO
- Agents

Intranet

- ポリシー管理
- ポリシー適合
- 連携ー Federation (IdP)
- Identity Web Services

Extranet

- Federation (SP)
- Identity Web Services

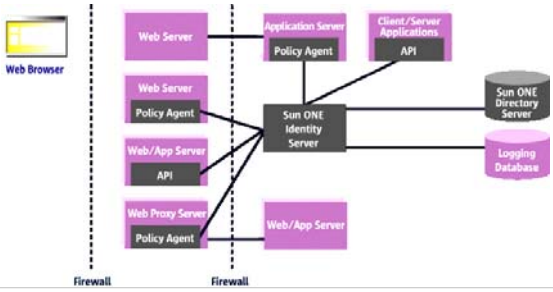
Access Manager の主な機能

- J2EE ベースのアーキテクチャ
- 認証サービス
- シングル・サインオン / セッションサービス
- 認可（ポリシー）サービス
- ポリシー・エージェント
- 監査・ロギングサービス
- 管理
- 連携サービス

 20

Web シングル・サインオン (SSO)

- エージェント型シングル・サインオン
  - Web Proxy Server の併用により リバース・プロクシ方式の SSO にも対応
- クロス DNS ドメイン Web SSO のサポート
- ワイルドカードによる保護リソースの指定
  - e.g. http://*.sun.com/*, http://www.sun.com/products/CA*



21

Sun Java System
Access Manager の優位点

- ユーザ / ポリシー情報のレポジトリを無料で提供
  - > Sun Java System Directory Server を内蔵
- 業界唯一の J2EE アプリケーションとして構築された認証システム
- SAML/Liberty による連携サービスいち早く実装
- 業界標準のサポート
  - > JAAS, SAML, Liberty, XML, Kerberos, OCSP, SPML
- 相互に連携 / 統合可能な包括的アイデンティティ管理製品群を提供
  - > LDAP データベース： Directory Server
  - > アクセス制御： Access Manager
  - > ユーザ情報のプロビジョニング： Identity Manager

22

Sun Java System Access Manager

- Access Manager 主要機能
  - 認証　(Authentication)
  - 認可　(Authorization)
  - 監査　(Audit)
  - ユーザ管理　(User Management)
  - 連携　(Federation)
- 製品コンポーネント
  - Access Manager Core
  - Directory Server
  - Policy Agent

Access Manager 主要機能

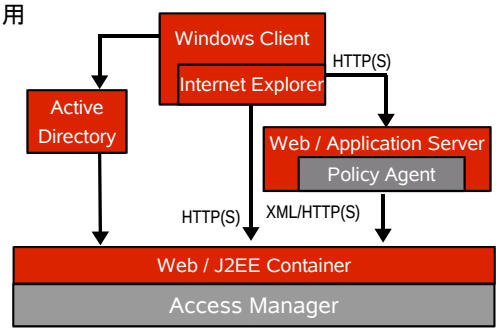
認証　(Authentication)

- 多彩な認証モジュールを提供
  - ID, Password による認証
  - X.509 デジタル証明書認証
  - Windows Desktop Single Sign-On
  - 新規自己登録認証
  - Anonymous 認証
- 認証方式の組み合わせによるセキュリティの向上
  - ２種類以上の認証の連結によりアプリケーションを保護
  - 特定のアプリケーションに対してはよりセキュリティレベルの高い認証を要求
- 認証クライアント API による認証
  - Java/C の API により、リモートアプリケーションの認証を Access Manager に委任することも可能

Access Manager 主要機能 > 認証 (Authentication)

Windows Desktop Single Sign-On

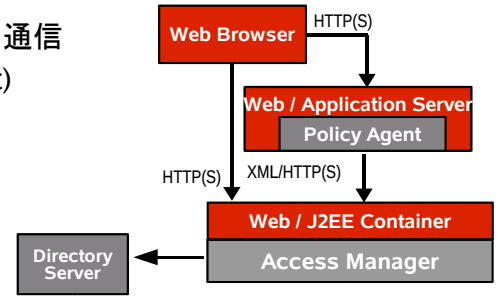
- Windows ドメインのログオンによる SSO
  - ユーザは Web ブラウザで ID, パスワードを入力することなくアプリケーションにアクセス可能
    - Windows ドメインにログオン
    - 保護されたアプリケーションにアクセス
    - ポリシーに基づいてアクセス権が付与
    - アプリケーションが認証されたユーザの属性情報を取得
    - 許可されたアプリケーションを利用
- Kerberos 認証
- Active Directory のパスワードを Directory Server に同期させる必要なし
- サーバは Windows 2000/2003 の Active Directory に対応
- クライアントは Windows Internet Explorer に対応



Access Manager 主要機能

認可 (Authorization)

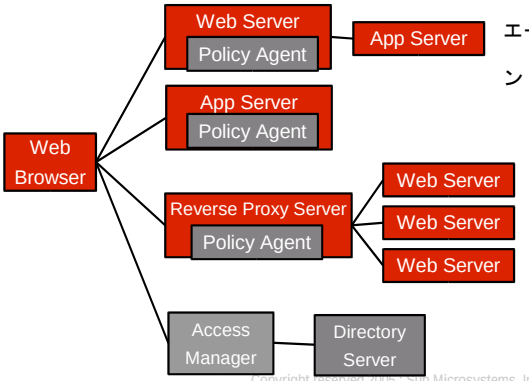
- 認可ポリシー
  - Access Manager 管理コンソールにより一括管理
  - Directory Server に格納
- Policy Agent
  - 認証 / 認可情報を XML/HTTP により Access Manager と通信
  - PEP(Policy Enforcement Point)
  - 既存アプリとの連携機能
  - セカンダリドメイン（クロスドメイン用） Cookie の生成



Access Manager 主要機能 > 認可 (Authorization)

Policy Agent

- アクセス制御対象サーバソフトウェアに導入されるモジュール
  - 実装は NSAPI, ISAPI, mod_xxx, J2EE Servlet Filter + Realm など
- エージェント型、リバースプロクシ型に対応



エージェント型
・クライアントが意識するアプリケーションのアクセス URL の変更が発生しない
・アプリケーションの内部で保持する「リンク」の URL に変更が発生しない

リバースプロクシ型
・既存システムに手を加える必要なし
・Web/App サーバに依存しない
・Sun Java System Web Proxy Server 3.6 及び Apache Web Server に対応

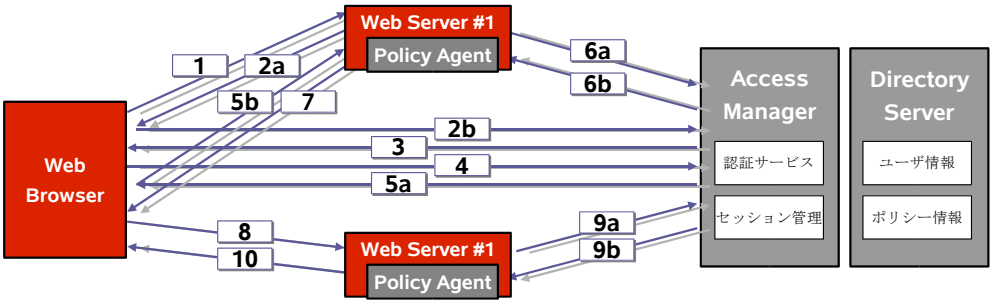
Access Manager 主要機能 > 認可 (Authorization)

対応エージェント (Policy Agent)

- Web Server
  - Sun Java System Web Server 6.0
  - Sun Java System Web Server 6.1
  - Apache Web Server 1.3.27
  - Apache Web Server 2.0.47
  - Apache Web Server 2.0.48
  - Microsoft IIS 5.0
  - Microsoft IIS 6.0
  - IBM HTTP Server 1.3.19
  - Oracle 9iAS HTTP Server
- Web Proxy Server
  - Sun Java System Web Proxy Server 3.6
  - Apache Web Server(Reverse Proxy Mode)
    - サポートバージョンは" Web Server" の項目を参照
- Application Server
  - Sun Java System Application Server 7.0
  - Apache Tomcat Application Server 4.1.27
  - JRun Application Server 4.0
  - IBM WebSphere 5.0
  - BEA WebLogic 6.1SP2
  - BEA WebLogic 7.0
  - BEA WebLogic 8.1
  - Oracle 9iAS Containers for J2EE
  - Oracle 10gAS Containers for J2EE
- その他
  - PeopleSoft 8
  - SAP Enterprise Portal 6 SP2 and Web Application Server 6.20 SP1
  - SAP ITS 2.0
  - Lotus Domino 5.0.12
  - Lotus Domino 6.0.1
  - Lotus Domino 6.5

Access Manager 主要機能 > 認可 (Authorization)

シングル・サインオンのフロー



1. **Web** サーバ **#1** 上のリソースにアクセス
   まだ認証されていない （トークンを持っていない） ので
   Access Manager に **HTTP** リダイレクト

2-4. 認証を要求するページを出力
   クリデンシャル **(e.g. LDAP** ユーザ名 およびパスワード）
   を入力

5a. 認証成功の場合 **Access Manager** 内のユーザ・セッション
   が有効化され， さらにトークンを **cookie** として付加し
   Web サーバ **#1** 上のリソースに **HTTP** リダイレクト

5b.Web ブラウザが Web サーバ #1 にトークンを提示

6. cookie として受け取ったトークンを
   Access Manager に送信

7. セッションの有効性とポリシー情報
   (URL パターン) を取得しアクセスが許可されるので
   あれば実際のコンテンツを出力

8. Policy Agent に対してトークンを提出

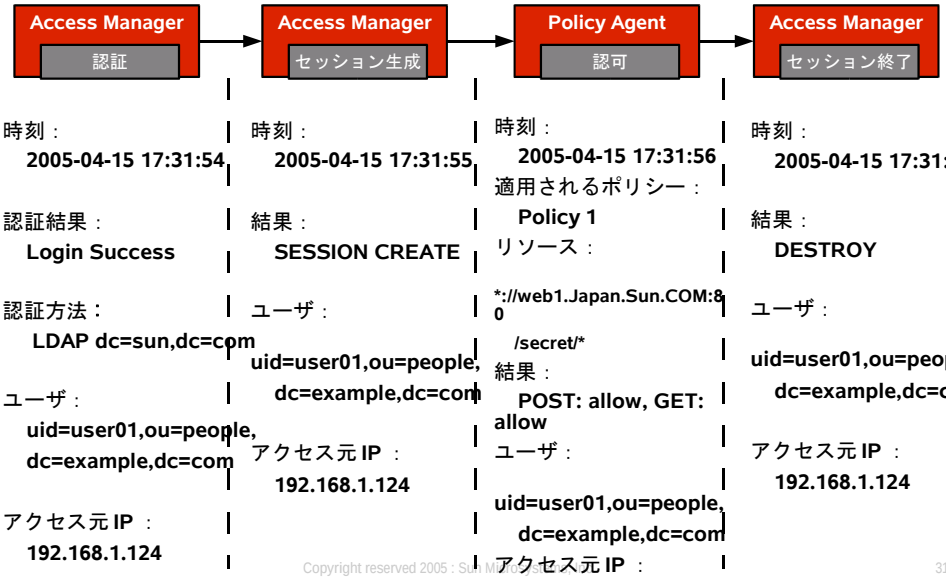
Access Manager 主要機能

監査 (Audit)

- 認証セッションのライフサイクルを監査
  - ログイン / ログアウト
  - アクセスの許可 / 拒否
  - 「いつ」「誰が」「どこから」「どのように（認証方法、適用されたポリシー）」を記録、追跡
- 管理者の行動を監査
  - ユーザ、ポリシー、認証機能の変更を監査
  - 作成、変更、削除までの流れを追跡
  - 「いつ」「誰が」「何を」「どこから」を記録
- ログの集中管理
  - Policy Agent へのアクセスを Access Manager 側で管理
  - DB(Oracle, MySQL など) への格納にも対応
- ログの改ざん防止
  - ディジタル署名 + MAC (Message Authentication Code)

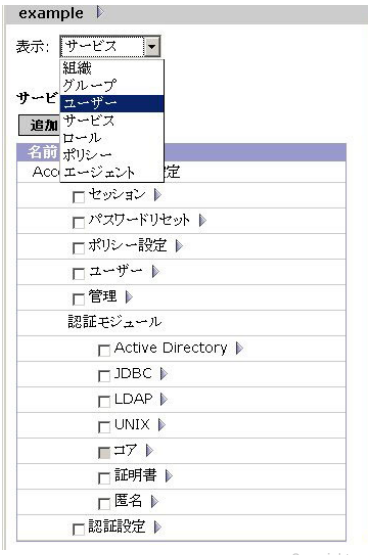
Access Manager 主要機能 > 監査 (Audit)

認証セッションのライフサイクルを監査



Access Manager 主要機能 > 監査 (Audit)

管理者の行動を監査



ユーザ管理
（例）
いつ： 2005-04-18 17:00:30
誰が： uid=amAdmin, ou=Peole, dc=example, dc=com
誰の： uid=user02, ou=People, dc=example, dc=com
何を：ユーザ uid=user02..... の属性 telephonenumber [03-5717-5000] -> [03-5717-5555] が変更されました
どこから： lab01.Japan.Sun.COM

ロール管理
（例）
いつ： 2005-04-18 18:00:30
誰が： uid=amAdmin, ou=Peole, dc=example, dc=com
何を： Created role cn=マネージャーロール , dc=example, dc=com
どこから： lab01.Japan.Sun.COM

ポリシー管理
（例）
いつ： 2005-04-18 19:00:30
誰が： uid=amAdmin, ou=Peole, dc=example, dc=com
何を：ポリシー Sample 用の... ルール Rule 2 を作成しました
どこから： lab01.Japan.Sun.COM

認証モジュール管理
（例）
いつ： 2005-04-18 20:00:30
誰が： uid=amAdmin, ou=Peole, dc=example, dc=com
何を： PlanetAMAuthLDAPService. iplanet-am-auth-ldap-user-search-attributes [uid]->[uid, cn] 用のサービステンプレートが変更されました
どこから： lab01.Japan.Sun.COM

Access Manager 主要機能

ユーザ管理 (User Management)

- 管理コンソール
  - Web ブラウザによりリモートから一元管理が可能
  - ユーザの作成 / 変更 / 削除
    - 管理する属性はカスタマイズ可能
    - 属性のアクセス権はカスタマイズ可能
  - ユーザのグループ化
    - グループ
    - ロール

- 管理権限の委譲
  - ユーザ / ポリシーの管理権限を委譲
  - セルフサービス
    - 許可された属性を自ら管理
    - パスワードリセット

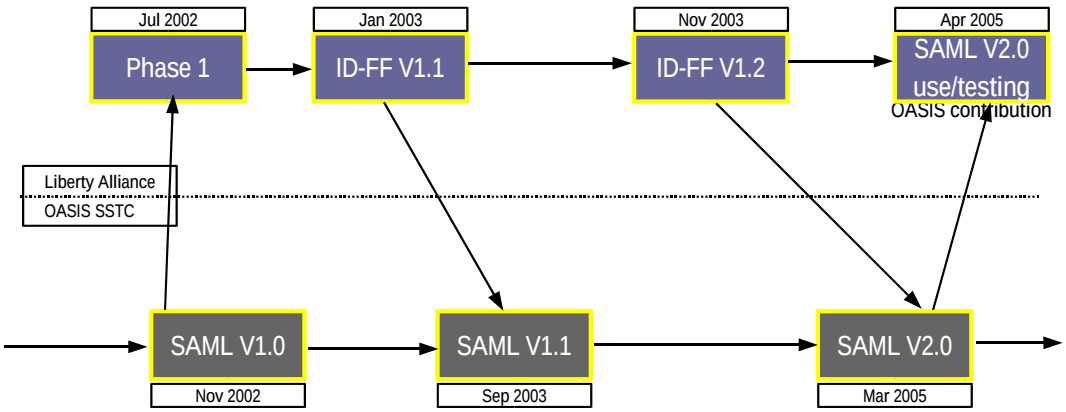
Access Manager 主要機能

連携 (Federation)

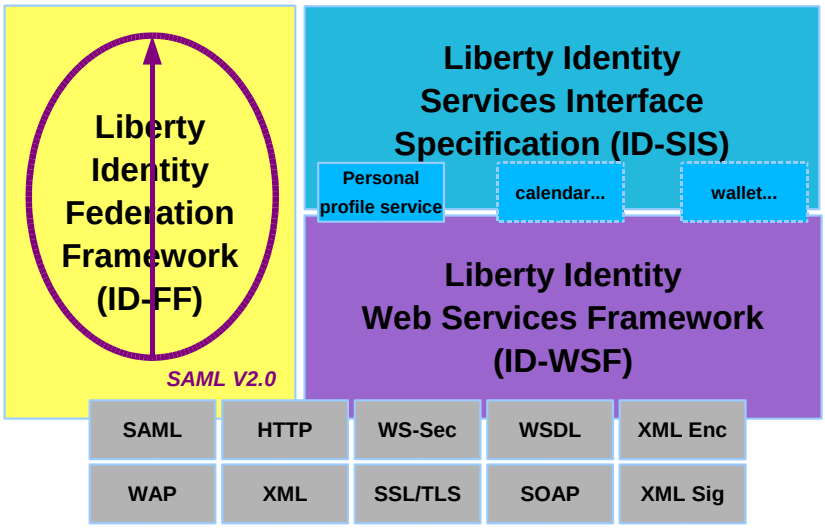
- SAML 1.1
- Liberty Phase-2 対応
  - ID-FF1.2
  - ID-WSF1.1
    - Discovery service
    - Interaction service
    - Authentication service
  - ID-SIS
    - Personal identityprofile (PIP)
    - Employee identity profile (EIP)

Identity federation の実装：時間軸と関係

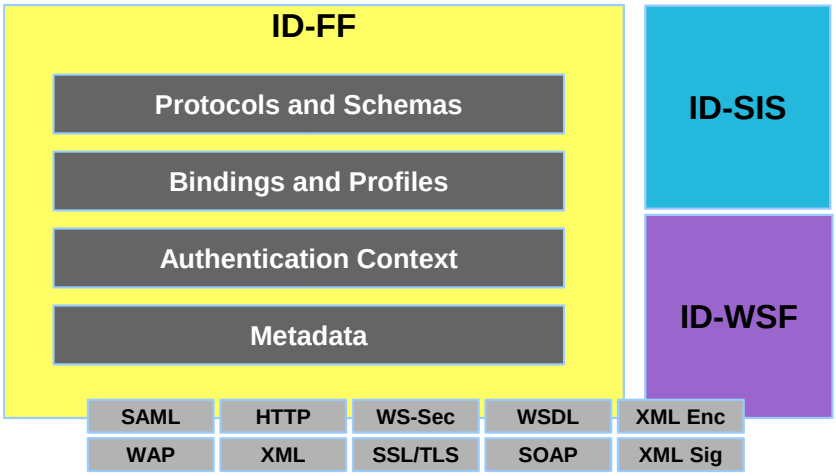
- 日付は最終仕様が決定した日



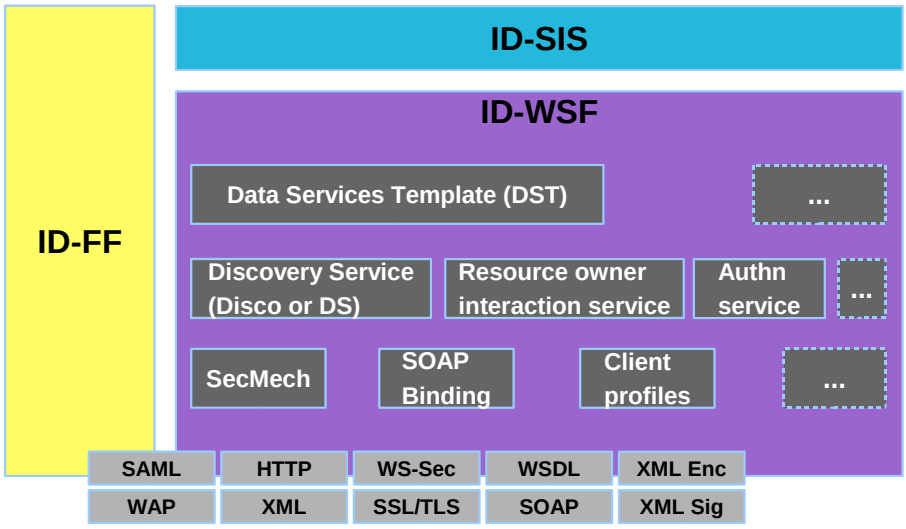
Liberty アーキテクチャのコンポーネント



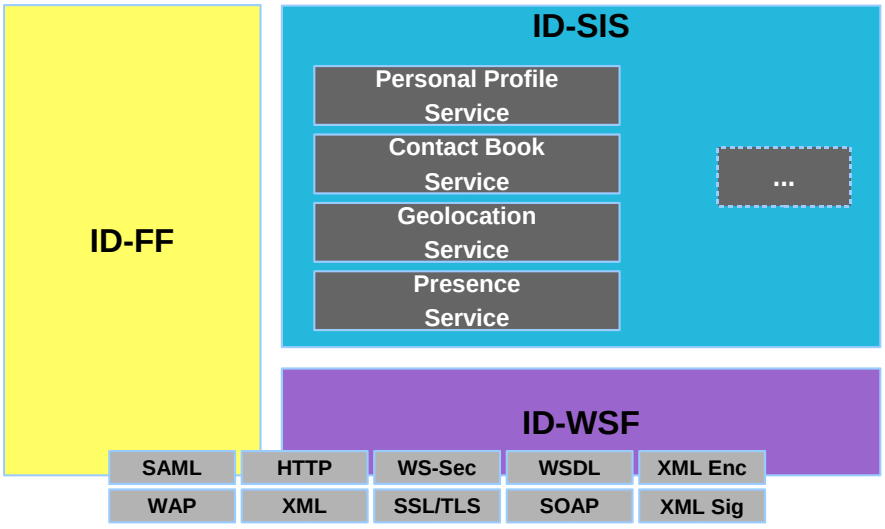
Liberty ID-FF の仕様



Liberty ID-WSF 仕様



Liberty ID-SIS 仕様

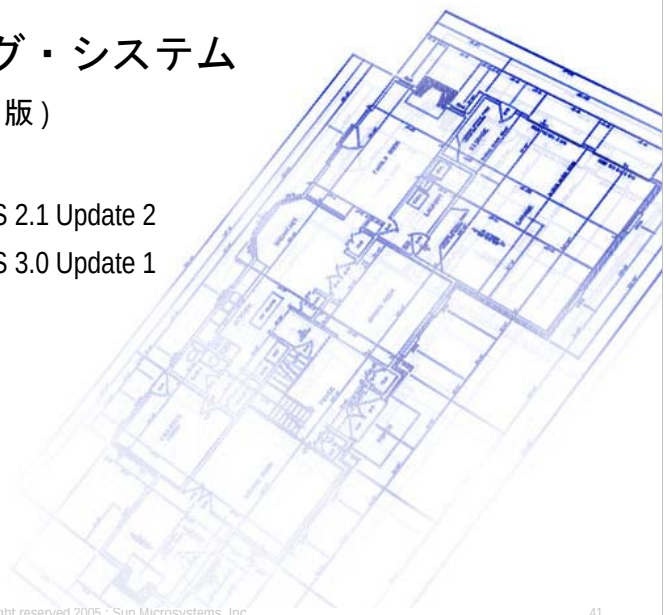


amSDK

- Access Manager SDK
- Access Manager の標準機能の拡張や新たなサービスの追加に利用
- 利用例：
  - SSO トークンからユーザの認証方式や認証状態などを取得
  - 独自ポリシー (例：データベースに格納された預金残高によりアクセス許可 / 拒否を決定) の作成
  - 独自認証モジュール (例：指紋認証) の作成
  - SAML による認証 / 認可情報の交換

ハードウェア / ソフトウェア要件

- オペレーティング・システム
  - Solaris 8, 9, 10 (SPARC 版)
  - Solaris 9, 10(x86 版)
  - RedHat Linux WS/AS/ES 2.1 Update 2
  - RedHat Linux WS/AS/ES 3.0 Update 1
- システム要件
  - メモリ : 512MB
  - ディスク : 250MB



リソース

- 製品概要
  - Access Manager
    - http://jp.sun.com/software/identity/access_mgr/
  - アイデンティティ管理製品全般
    - http://jp.sun.com/javasystem/index.html
- 製品ドキュメント
  - docs.sun.com にて提供
  - http://docs.sun.com/app/docs/prod/entsys#hic
- 評価版ダウンロード (無料)
  - Download Center にて提供
  - Java Enterprise System に含まれます
  - http://www.sun.com/software/javaenterprisesystem/get.xml

新技術続出：アイデンティティが中心

- 見落としてはならない主な仕様
  - > SSO および認証フレームワーク関連
    - > SAML, ID-FF, WS-Federation, (WS-*),XKMS,XML signature
  - > アイデンティティ Web サービス
    - > ID-WSF,ID-SIS
  - > アクセス・コントロール
    - > XACML
  - > プロビジョニング
    - > SPML
  - > ディレクトリ
    - > DSML

新時代の幕開け：技術の一貫性

インターオペラビリティが中心