



Sun Java System Directory Server Enterprise Edition 6

新機能および製品概要のご紹介

ver. 2007/01/12

サン・マイクロシステムズ株式会社
Sun Javaソフトウェア統括本部

アジェンダ

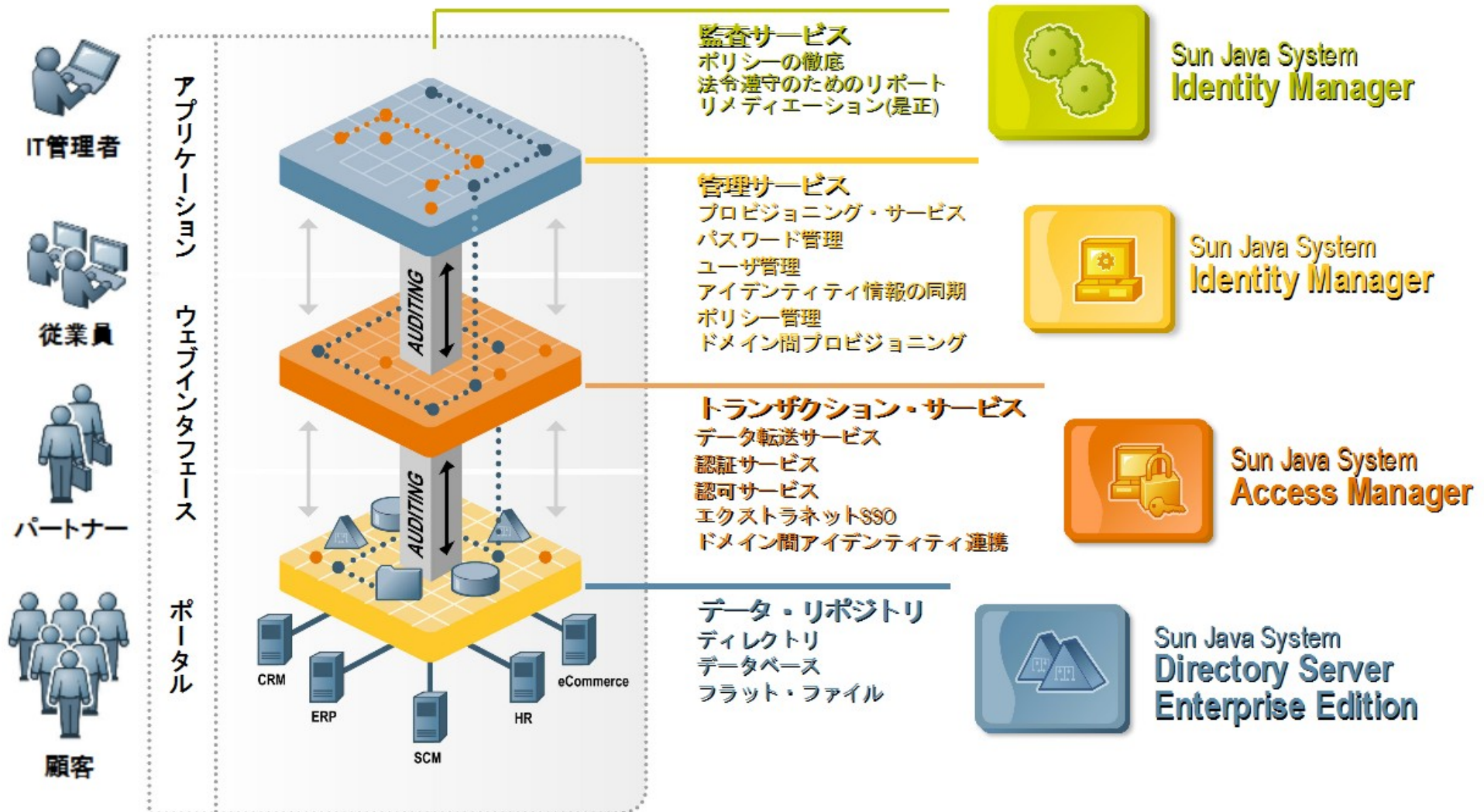
- 
- はじめに
 - > Sun の IdM ソリューション
 - > Directory Server Enterprise Edition
 - 製品コンポーネント紹介
 - > Directory Proxy Server
 - > Directory Server
 - > Identity Synchronization for Windows
 - > その他のコンポーネント
 - Directory Editor
 - Directory Server Resource Kit
 - ご参考

はじめに

Sun の IdM ソリューション

Sunのアイデンティティ管理ソリューション

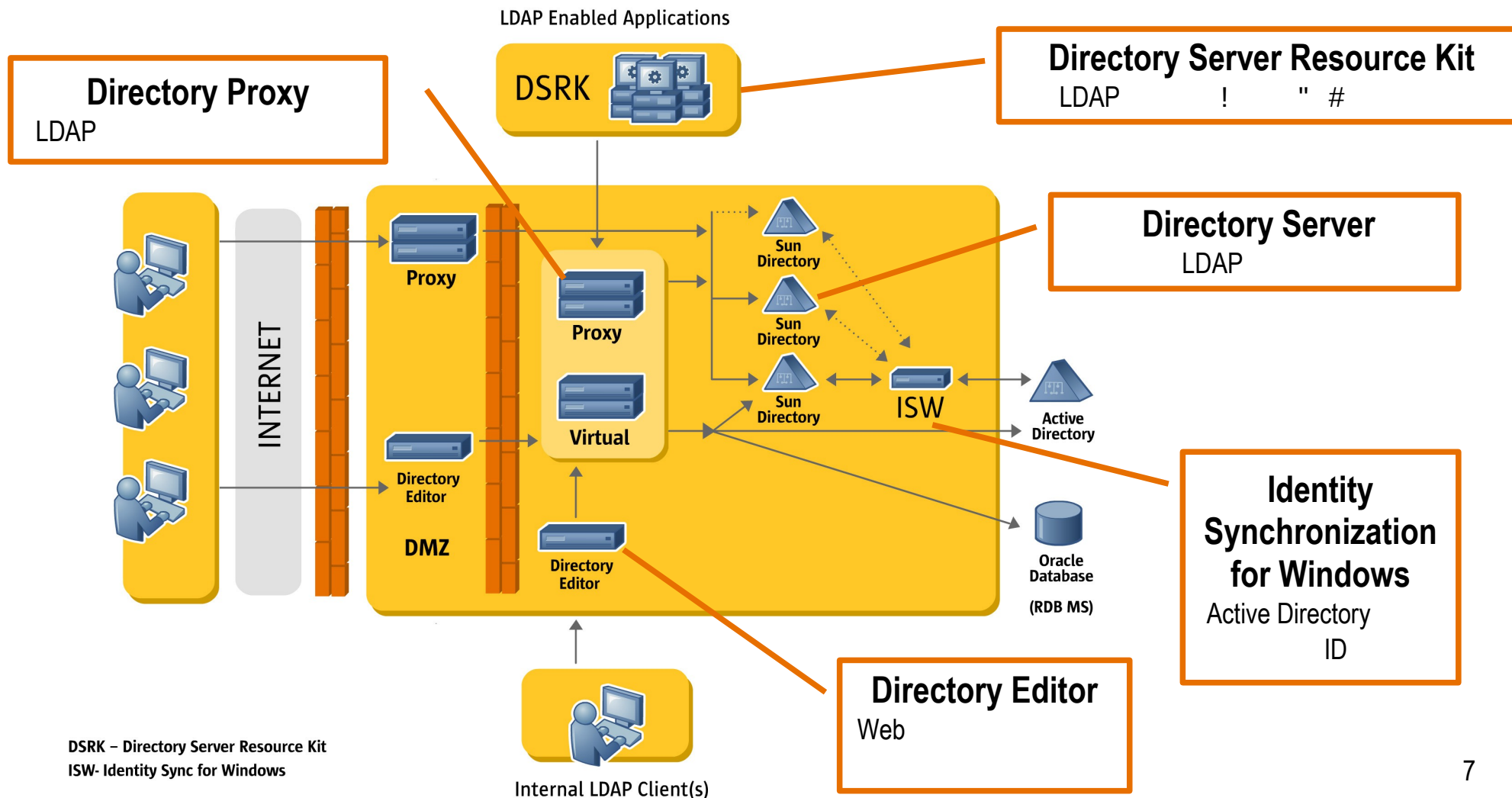
- ディレクトリサービスはアイデンティティ管理の根幹



Directory Server Enterprise Edition

Directory Server Enterprise Editionとは

- Directory Server 及び Directory Server をより活用するためのソフトウェアを含めた統合パッケージ



Directory Server Enterprise Editionの特長

- 誕生から 10 年、30 億エントリ以上の実装実績
 - > Fortune 100 の企業のうち少なくとも 40 社以上にて利用
- エントリレベルのサーバでも高性能を発揮
 - > 例: 秒間 6800 回を超える認証 / SunFire T2000 (1CPU8core) / Solaris / 25 万ユーザ)
 - http://blogs.sun.com/DirectoryManager/entry/sun_t2000_vs_dell_68501
- 細かな制御により強固なセキュリティを確保
 - > 属性の暗号化、属性レベルでの ACI
- LDAP ディレクトリ単体だけではなくディレクトリ・ソリューションを提供
 - > バックエンドデータベースの仮想化 / フィルタリングを実現する Directory Proxy Server
 - > Active Directory とのアイデンティティ同期を実現する Identity Synchronization for Windows

Directory Service Control Center

- Directory Server Enterprise Edition (DSEE) コンポーネントを統合管理するために用意された Java Web Console ベースのツール
- Web ブラウザのみでユーザ管理から詳細な設定まで実行可能
- 主な機能
 - > ユーザ管理
 - > サービスの追加 / 設定
 - > サービスの起動 / 停止
 - > アクセス監視、エラー監視
 - > パフォーマンスチューニング
 - > バックアップ / リストア
- 管理用のコマンドラインツールも新たに提供



DSCCによる管理全体像(アーキテクチャ)

dsconf

```

/      &      '
Directory Server01 23
LDAP      ,% 4
56 78 /      ()* +
,      -!.
    
```

dpadm

```

$% &      '
Directory Proxy Server
() *+ , -!.
    
```

dsadm

```

$% &      '
Directory Server
() *+ , -!.
    
```

Console Agent

```

Directory Server/Directory
Proxy Server9 ;; ()
<      ' 4: ;2=
><      ?      ()
,-      !.?      @A
    
```

Directory Service Control Center

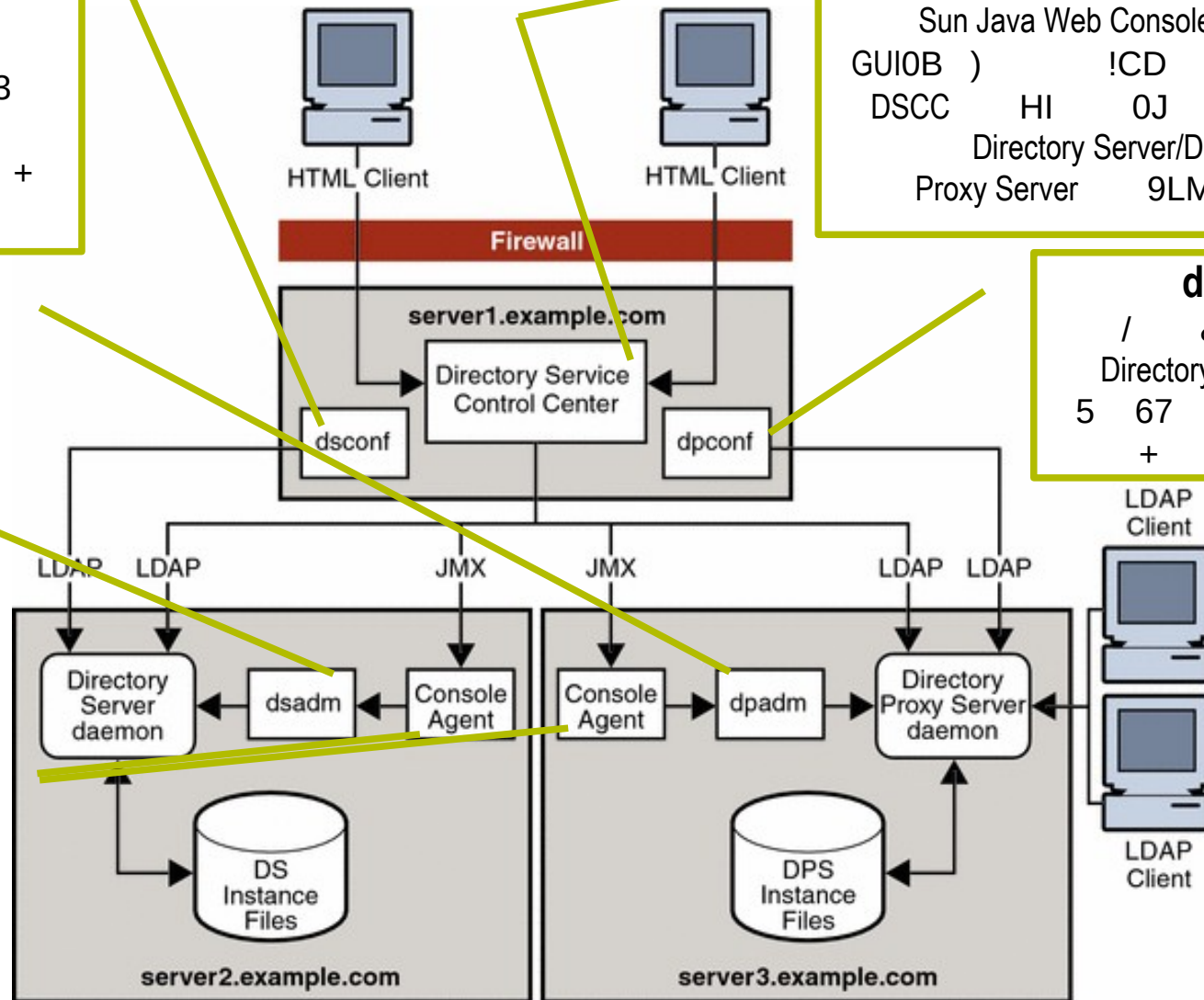
```

Sun Java Web Console
GUI0B )      !CD E      ?F G
DSCC      HI      OJ      1K
Directory Server/Directory
Proxy Server      9LM NO)
    
```

dpconf

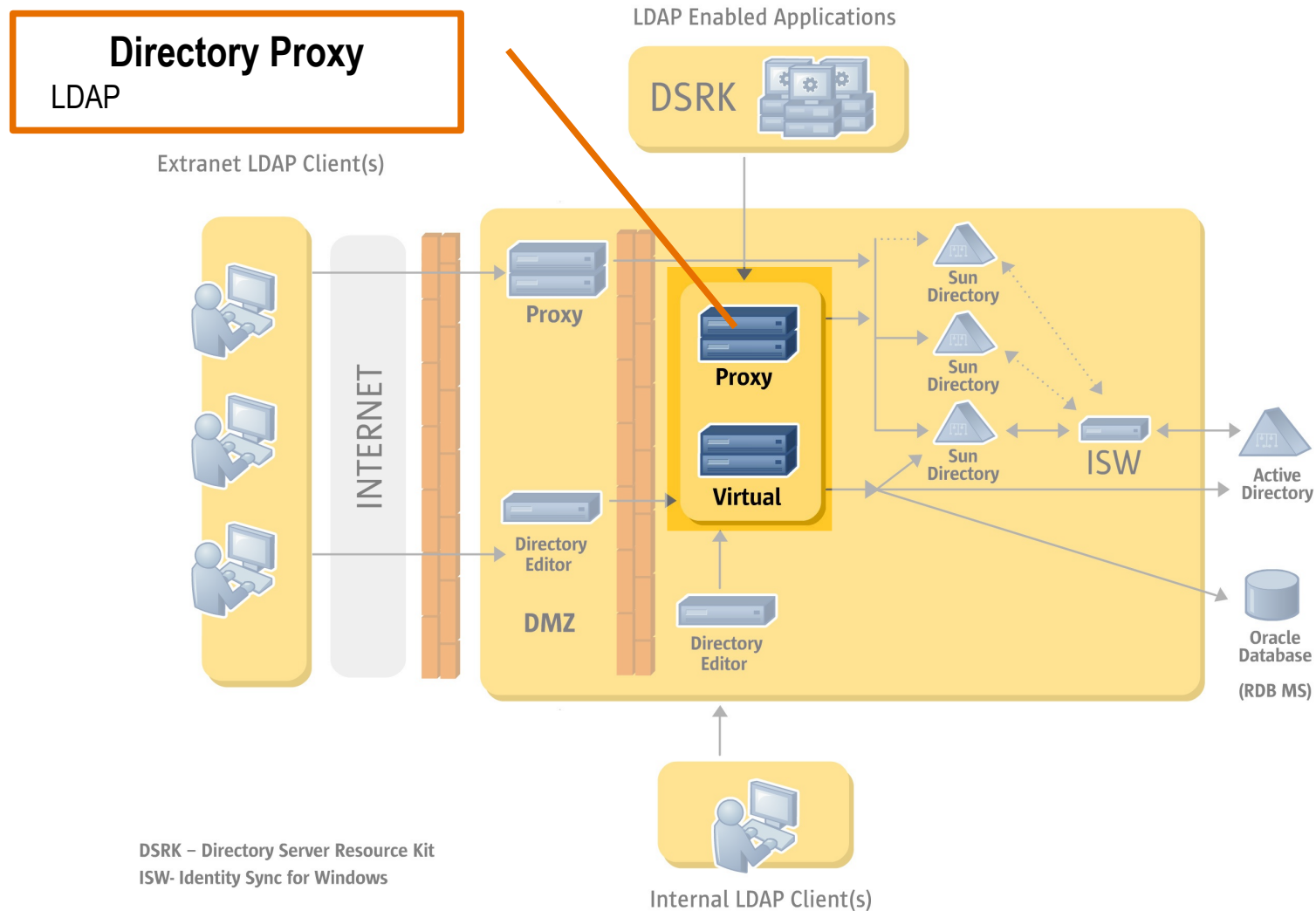
```

/      &      '
Directory Proxy Server
5 67 8 /      ()*
+ , - !.
    
```



Directory Proxy Server 6.0

Directory Proxy Server

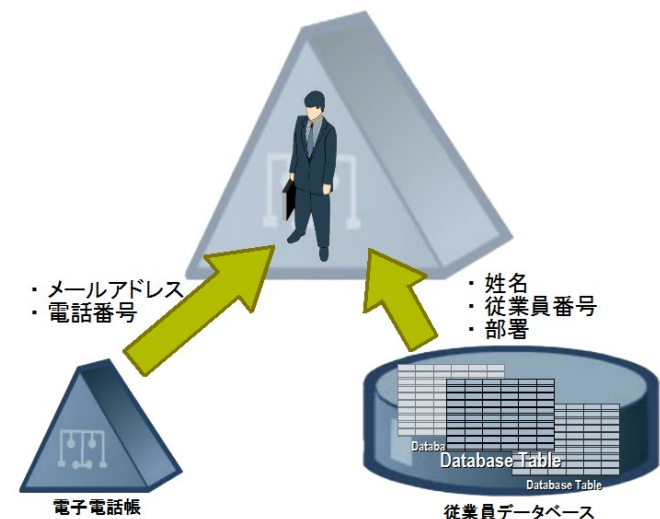
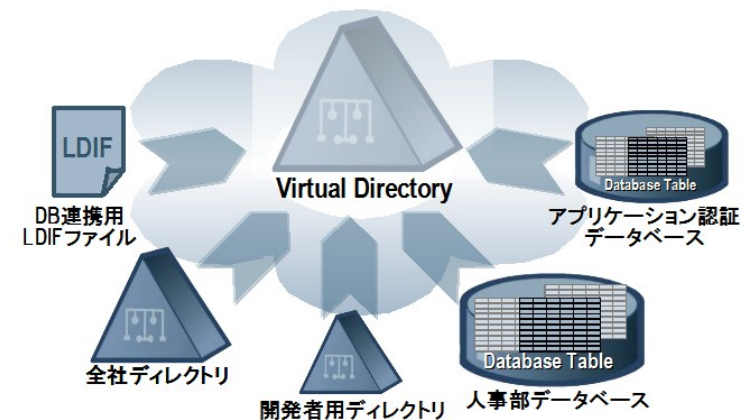


Directory Proxy Server の主要機能

Directory Proxy Serverの主要機能

データベースの仮想化(Virtual Directory)

- 複数異種データベースの一元的なビューを提供
 - > LDAP サーバ / JDBC 対応データベース / LDIF ファイルに対応
 - > ビューはLDAP のインタフェースを提供
 - > データベースに存在する複数のデータベーステーブルから1つのビューを作成することも可能
 - > 異なるタイプのデータベースに分散された断片的情報を統合した'エントリ'の構成が可能
 - > ビューに対して書き込みも可能
- 仮想化された View にも ACL の設定が可能
 - > Virtual ACLs

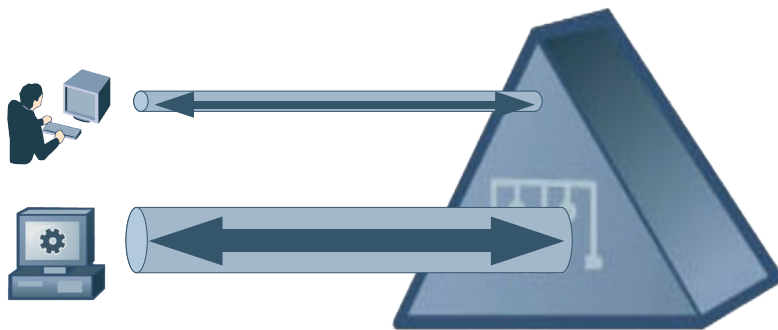


Directory Proxy Serverの主要機能 アクセス制御

- クライアントに応じたオペレーションの制限

- > リソース制限ポリシー

- 最大接続数
 - 最大オペレーション数
 - 検索範囲
 - 検索時間
 - 検索サイズ
 - etc...

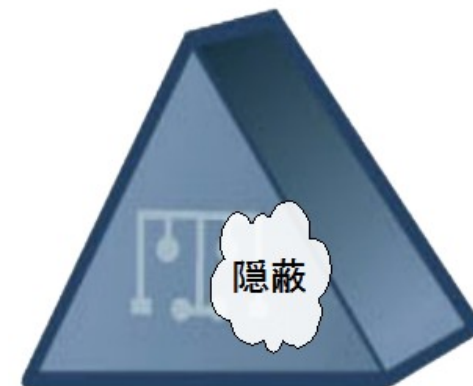


予め登録された特定のクライアント以外からの接続を制限

- クライアントに応じた情報の開示 / 隠蔽

- > 要求フィルタリングポリシー

- LDAP クライアントの IP アドレスや BIND ユーザに応じてサブツリーの開示 / 隠蔽が可能
 - エントリ単位、もしくはエントリの属性単位レベルで開示 / 隠蔽が可能

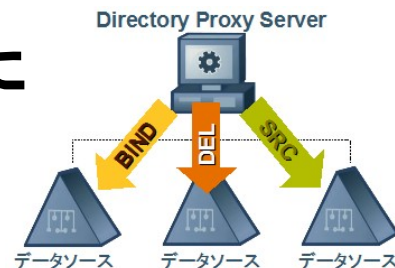


Directory Proxy Serverの主要機能

LDAPに特化したルーティング/負荷分散

オペレーションによる振り分け

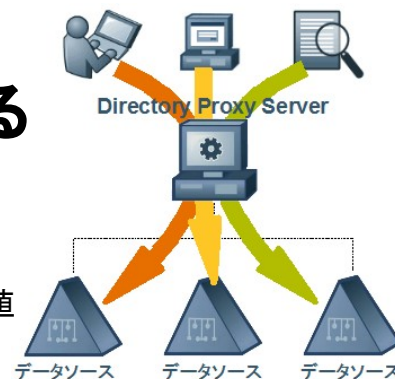
Bind, Add, Search, Delete, Modify,,,etc



- Bind処理を常に同一サーバに振り分けることで一定回数以上のBind失敗によりアカウントをロックアウト（グローバルロックアウトとの併用）
- 同一クライアントから同一エントリに対する検索処理を同一サーバに振り分けることでキャッシュを最適化

ハッシュ値による振り分け

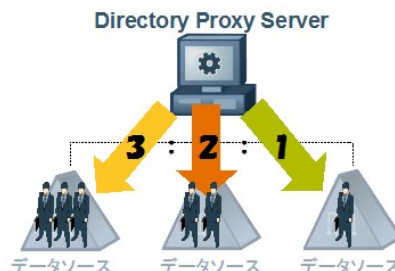
リクエストタイプやリクエストプロパティに応じてハッシュ値を付与



- 連続的な書き込み（後処理が前処理の結果に依存する場合）への確実な対応
- 重み付けも可能
- 閾値に設定すると特定のサーバに対する負荷が増加（例：特定 DN でのBIND処理は常に同一サーバに転送されることになる）

重み付けによる振り分け

50:50, 40:30:30,,,etc

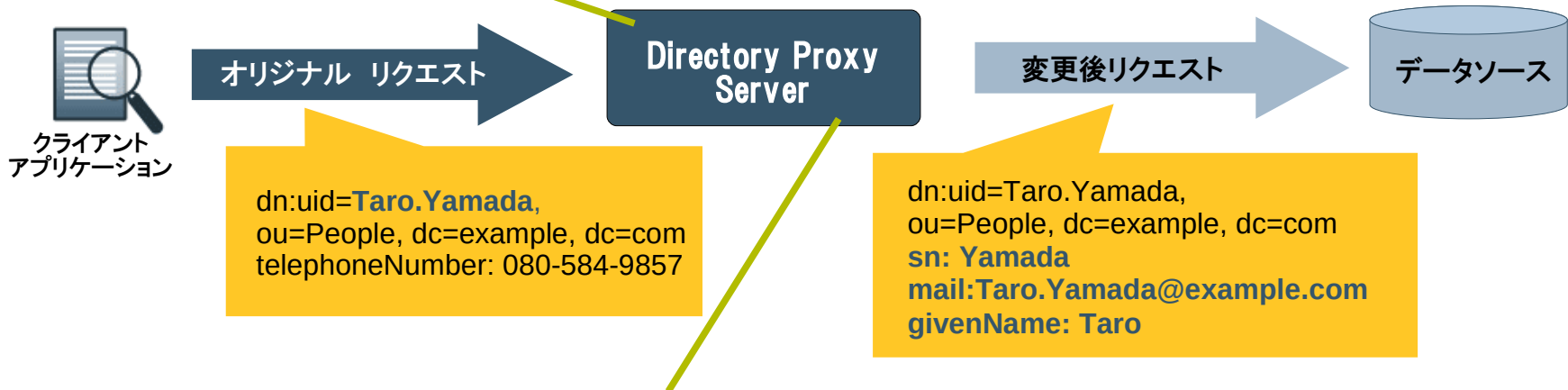


- 100% - 0% に設定することでフェイルオーバーを実現
- サーバの処理能力に応じた負荷分散

Directory Proxy Serverの主要機能

属性/属性値/ユーザの置換機能

- > クライアントアプリケーション / データソースに合わせてリクエスト内容を動的に変更
 - 属性置換 / 生成 / 削除
 - 属性値の生成 / 変更 / 削除
 - 固定値の埋め込み / 値の増減 / 部分文字列の抜き出し / 文字列の分割 / 値の結合



- > 接続ユーザを別ユーザに変換(マッピング)して処理を実行することも可能

Directory Proxy Serverの主要機能

データソースの監視と警告

- 監視方法

- > Lv.1: プロキシとデータソース間の通信エラーを検知
- > Lv.2: 定期的にデータソースと通信を実施
 - 一定期間通信が行われない場合のみ
- > Lv.3: 既存のコネクションを利用して ping (Search リクエスト) を実施
 - e.g. Active Directory からのコネクションの切断を防ぐために利用



- 障害検知時の対応

- > コネクションを切断し、再接続を実施
- > 再接続に失敗した際には障害フラグを立て、すべてのコネクションを切断
- > 他のデータソースに対して自動的にリクエストを投げ直す
- > 投げ直し先が存在しない場合はエラーをクライアントに返す
- > データソースが回復した場合には自動的にフェイルバック

- 警告の送信

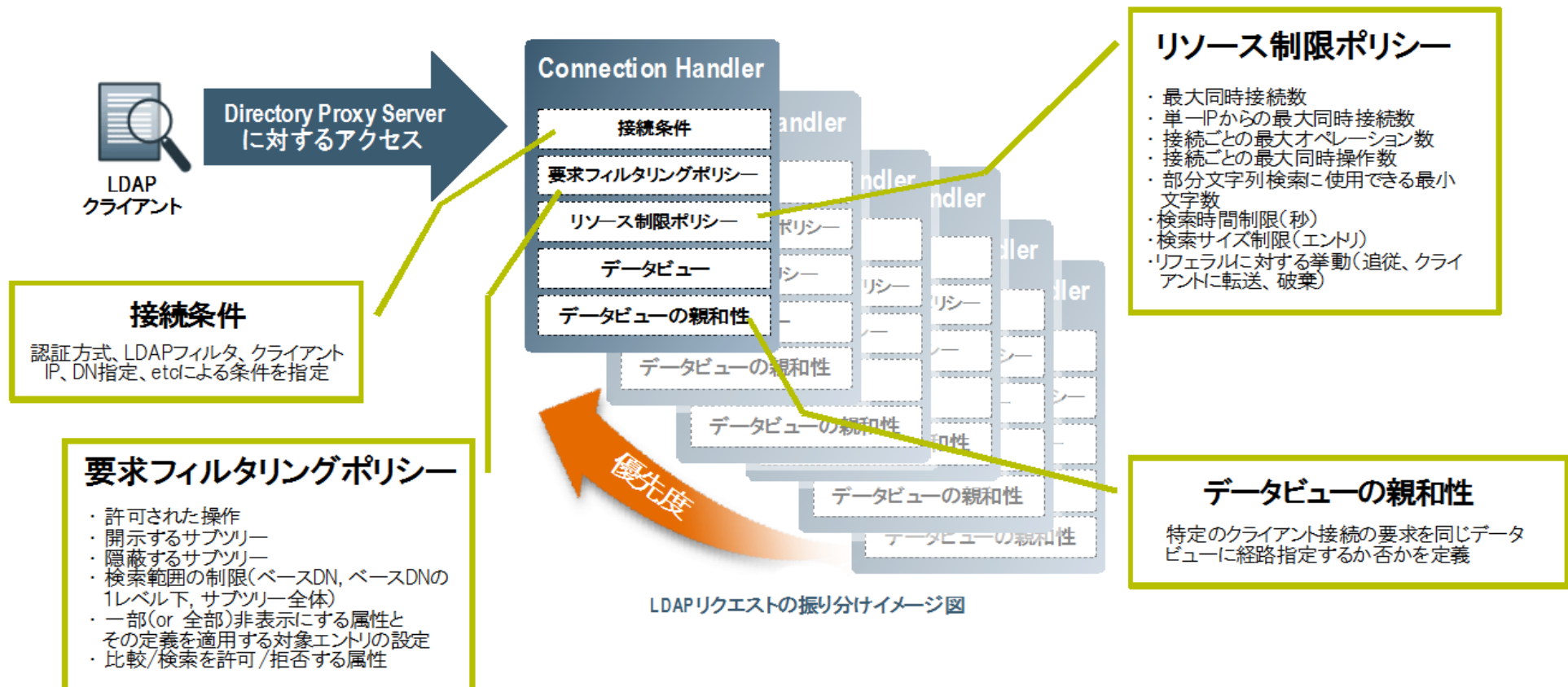
- > Syslog 出力、電子メール、スクリプト実行

Directory Proxy Server のアーキテクチャ

Directory Proxy Serverのアーキテクチャ

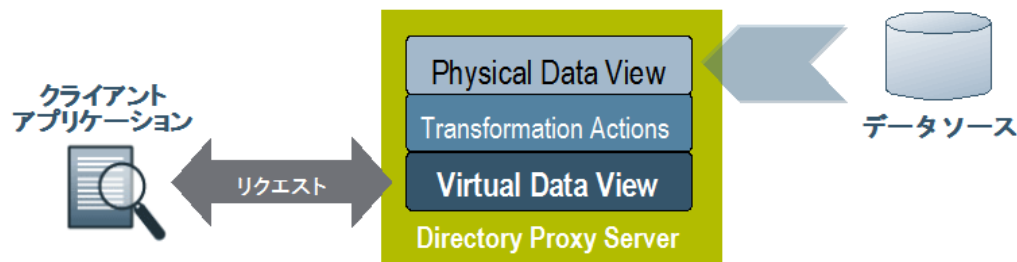
Connection Handlerによる制御

- 接続コンテキストに基づいて割り当てられるハンドラがアクセス制御やルーティング方法を決定
- Connection Handler は優先順位に基づいて決定される



Virtual Data Viewの生成

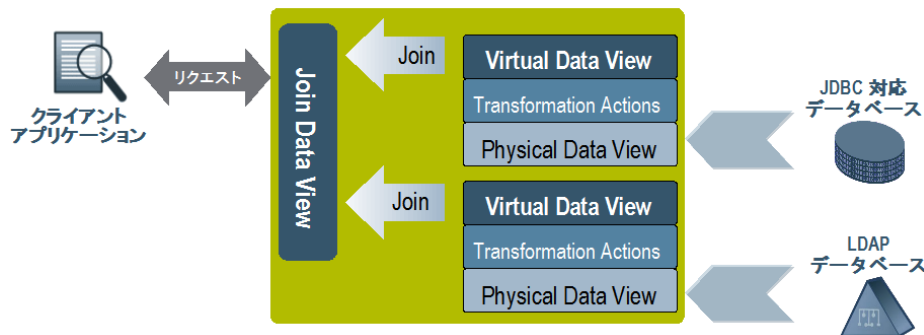
- 物理的なデータベースから論理的なデータベースを構築
 - > 変換処理 (Transformation Actions) を Data View に適用可能
 - 属性 / 値のカスタマイズ (カスタマイズ可能な内容は「属性 / 属性値 / ユーザの置換機能」のスライドを参照) 内容をビューに追加
 - 例: ADAM の objectclass 'user' を inetOrgPerson に置換
 - 例: メールアドレスを uid 属性値と文字列 '@example.com' を組み合わせ作成
 - 読み取り時のみだけでなく書き込み時の変換も可能



- > ビューに対する制限
 - 属性単位で設定
 - 参照不可能 / 可能、書き込み不可能 / 可能な属性の指定

Join Data Viewの生成

- 異なる Data View から一つのビューを構築
 - > Join Rule に基づく Primary Data View と Secondary Data View の統合
 - DN Join Rules
 - DN の一部が同じであるエントリを統合
 - ou=People 以下のエントリで cn 属性値が同じエントリを統合する場合
`cn=${primary-data-view.cn},ou=people`
 - Filter Join Rules
 - 統合するエントリを検索するためのフィルタを定義
 - 社員のエントリに組織情報のエントリをマージする場合
`departmentnumber=${departmentnumber}`



Virtual Data ViewからJoin Data Viewを構築

- > Transformation Actions の適用も可能

その他

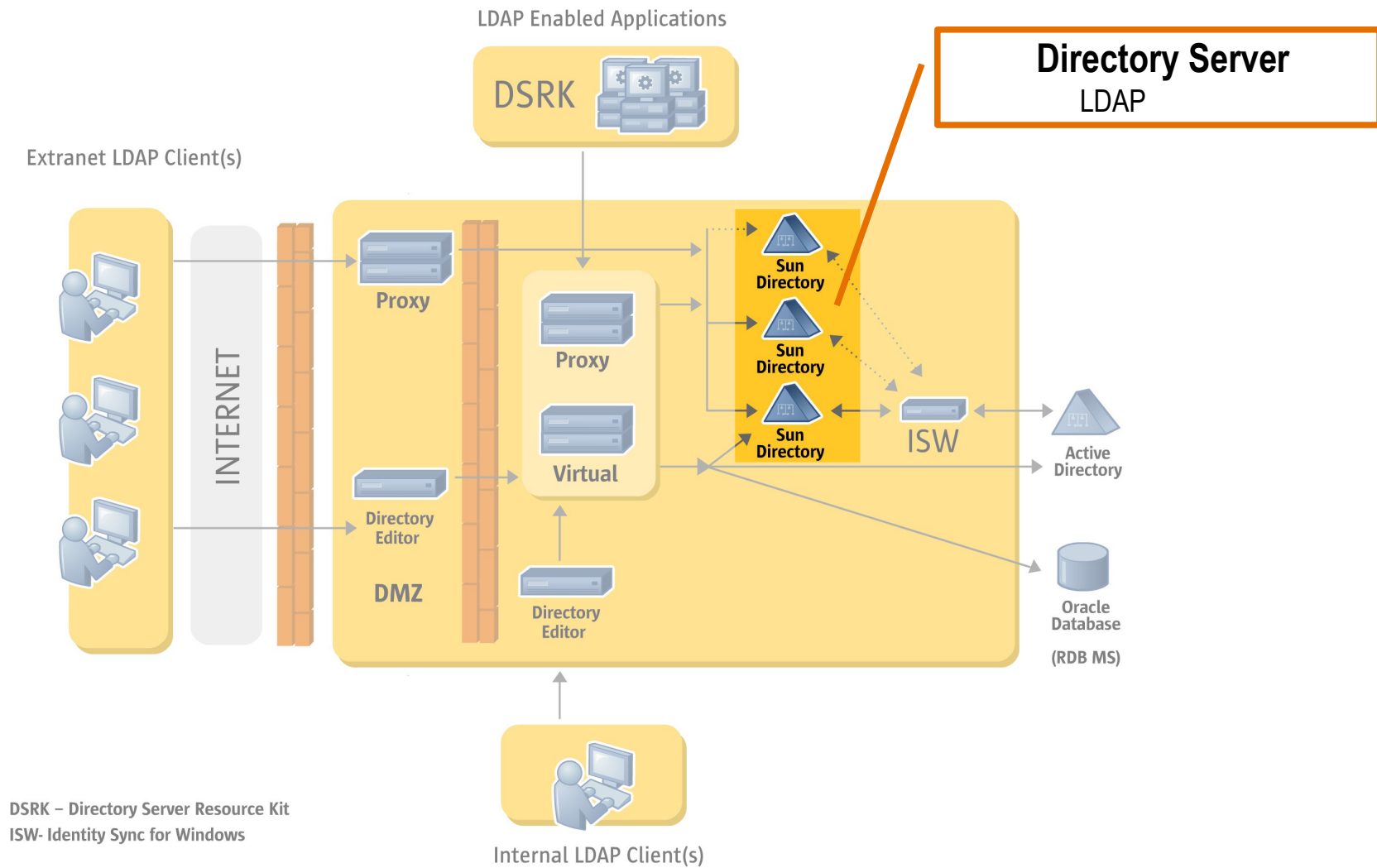
Directory Proxy Server 対応プラットフォーム



- Solaris
 - > 10 (SPARC, x86)
 - > 9 (SPARC, x86)
- HP-UX 11.11 (PA-RISC 2.0)
- Red Hat Advanced Server 3.0 U4 (x86), 4.0 U2 (x86)
- Microsoft Windows
 - > 2000 Server SP4
 - > 2000 Advance Server SP4
 - > 2003 Server Standard Edition SP1, Enterprise Edition SP1
- 対応プラットフォームは予告なく変更される可能性があります
- 最新の対応状況については製品ドキュメントをご参照下さい

Directory Server 6.0

Directory Server



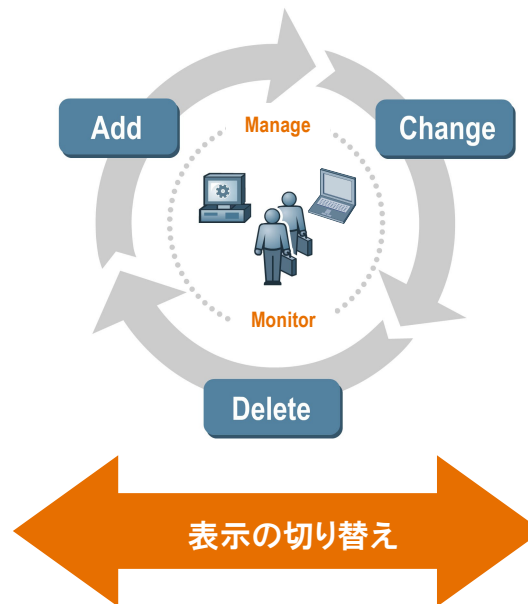
Directory Server の主要機能

Directory Serverの主要機能

DSCCによるエン트리管理

- Web ブラウザだけで複数のサーバにまたがるエントリを一括管理
- フォーム形式 / テキストビューによりエントリの管理が可能

フォーム形式



テキストビュー

エントリのグループ化

- グループ
 - > エントリをまとめるためのメカニズム
 - 種類: 静的グループ、動的グループ
- ロール
 - > グループを機能的 / 性能的に進化させたメカニズム
 - メンバのエントリを参照するだけで所属するロールが判明
 - 種類: 管理されたロール、フィルタを適用したロール、入れ子状のロール



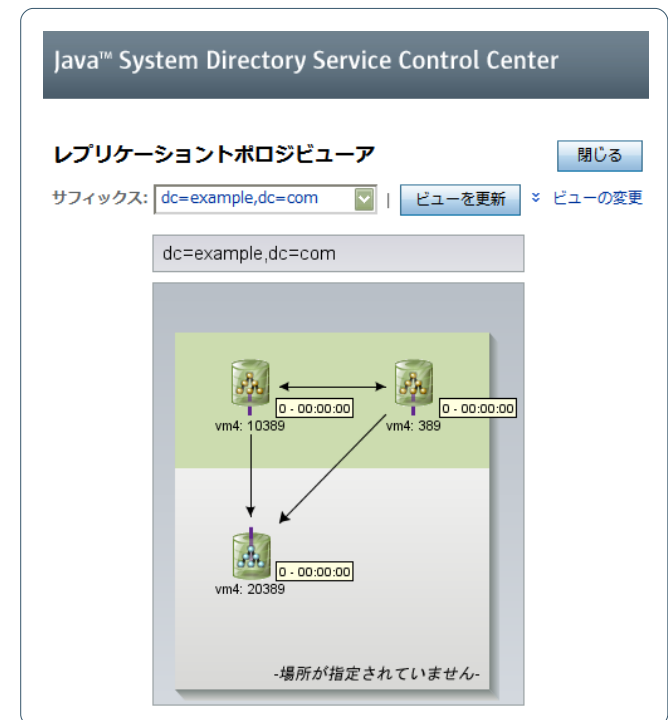
- サービスクラス (CoS)
 - > エントリに対して仮想属性を動的に割り当て
 - e.g. ユーザの部署コードを「上司と同じ」になるよう設定しておくで上司と同じ部署コードが属性として割り当てられる(上司を変更すると自動的に部署コードも変更される)

	グループ	ロール
静的(メンバを直接指定)なグルーピング	○(静的グループ)	○(管理されたロール)
動的(メンバをフィルタにより指定)なグルーピング	○(動的グループ)	○(フィルタを適用したロール)
メンバ対象範囲の限定	× (ディレクトリ全体がメンバ対象範囲)	○(ロールエントリの親エントリの配下がメンバ対象範囲)
メンバエントリへのメンバフラグの動的な付与	△(静的グループのメンバに対して isMemberOf属性が付与される)	○(管理されたロールのメンバはnsRoleDN属性を持ち、さらにすべてのロールのメンバに対してnsRole属性が付与される)

Directory Serverの主要機能

マルチマスタ・レプリケーション

- 無制限にデータベースのレプリケーションを作成可能
- レプリケーショントポロジビューワ
 - > レプリケーションの設定状況をグラフィカルに表示
 - > レプリケーション処理の遅延状況をレプリケーションごとに表示
- 複製処理の優先付け
 - > 処理種別(追加 / 変更 / 削除)
 - > 処理のオーナー
 - > 処理対象(サフィックス、属性)
- 対象となる属性のフィルタリング
 - > 特定の属性のみをレプリケーション
- タイミングの制御
 - > リアルタイム、週単位 / 時間帯指定
- ツリーの部分的なレプリケーションも可能
- WAN 越えのレプリケーションにも対応



レプリケーショントポロジビューワ

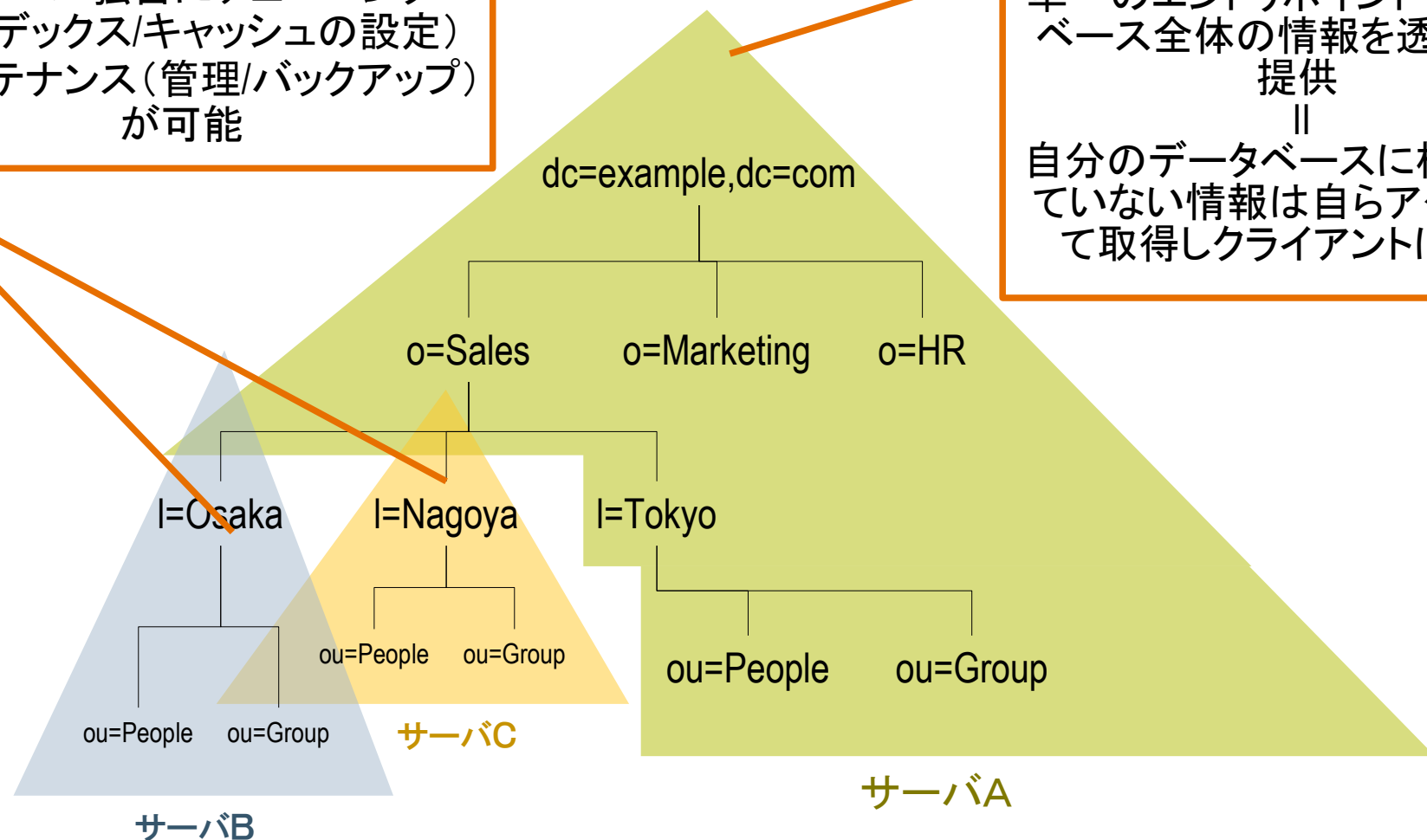
Directory Serverの主要機能

連鎖機能を用いた分散管理

各サーバ独自にチューニング
(インデックス/キャッシュの設定)
やメンテナンス(管理/バックアップ)
が可能

単一のエントリポイントでデータ
ベース全体の情報を透過的に
提供

||
自分のデータベースに格納され
ていない情報は自らアクセスし
て取得しクライアントに返却



その他セキュリティに関する機能

- 属性レベルでの ACI の設定が可能
 - > 接続 (BIND) ユーザ、曜日 / 時刻、クライアント IP アドレス
 - e.g. Anonymous でのアクセスではメールアドレスは検索できても電話番号は検索できない
 - e.g. あるアプリケーションからの認証リクエストは 9 時 ~ 17 時までの間しか受け付けない
- 細かなパスワードポリシー
 - > パスワード変更の強制ルール (変更頻度、ユーザによる変更の許可 / 拒否、変更時に旧パスワードの入力を求める ...etc)
 - > 暗号化方式 (平文、SSHA、SHA、Unix...etc)
 - > パスワード強度の設定 (大文字 / 小文字の使用を強制、特定用語の使用禁止、最小文字数 ..etc)
 - > アカountのロックアウトポリシー
- グローバル・アカウントロック
 - > 度重なる認証失敗によりアカウントロックされた情報もレプリケーションの対象



その他

Directory Server 6 の主な新機能



- Web ベースの管理インタフェースの導入
- グローバルアカウントロックアウト
 - > アカウントのロックアウト情報を複製することが可能
- CLI による管理性の向上
 - > Directory 管理のコマンド(インスタンス作成、レプリケーションの有効化など)が追加
- 複製機能の進化
 - > 複製数の制限を除去、優先順位付け、Retro Change Log の複製に対応
- セキュリティの向上
 - > パスワードなしのバインド拒否、パスワードリセット後のパスワード変更を強制、複数のスーパーユーザ作成に対応、より細かなパスワードポリシー等
- Frozen Mode の導入
 - > データベースの更新を停止し、安全にバックアップの取得が可能

評価・実績

- 30億エントリ以上の実装実績
- 第三者評価機関による評価
 - > <http://jp.sun.com/newsletters/innercircle/0507/feature4.html>
 - Gartner の Directory Server Magic Quadrant で第 1 位
 - Radicati Research の調査でマーケット・シェア第 1 位
 - Burton Group の調査でマーケット浸透度第 1 位
- 業種別の実績
 - 金融機関上位 10 社すべて
 - 通信サービス上位 10 社のうち 8 社
 - 無線通信サービス上位 10 社のうち 7 社
 - 自動車メーカー上位 10 社のうち 7 社
 - 航空宇宙・防衛分野の上位 10 社のうち 6 社
 - 航空会社上位 5 社のうち 3 社
 - 製薬会社上位 10 社のうち 7 社



Directory Server事例紹介

SINA Corporation



ポータルを支える1.2億エン트리収容バックエンドデータベース

• SINA Corporation とは

- > 中国及び世界中の中国コミュニティのためのオンラインメディアカンパニー
- > 2.3 億登録済みユーザ、6 千万有償サービスユーザを抱える ISV
- > 4.5 億ページビュー / 日にも及ぶニュース、携帯向けサービス、企業向けサービス、オンラインショッピングサービス ...etc を提供

• ビジネス要件

- > パフォーマンス(大規模「現在 1.2 億エン트리、将来的に 6 億エン트리まで拡張」に耐え得る製品)
- > サーバの運用費削減
- > 消費電力と設置面積の抑制

• Sun のソリューション

- > 30 台の Dell 製 Xeon ベース Linux サーバを 12 台の Sun Fire T2000/Solaris 10 サーバでリプレイスすることで**5倍の性能・1/4 のスペース・1/7 の消費電力**を達成



“The Sun Fire T1000 server's CoolThreads and multi-core technology and support for the 'Green Computing' standard set a milestone for the entire Internet service industry.”

— Li Songbo, Chief Technology Officer, Sina

<http://www.sun.com/customers/servers/sina.xml>

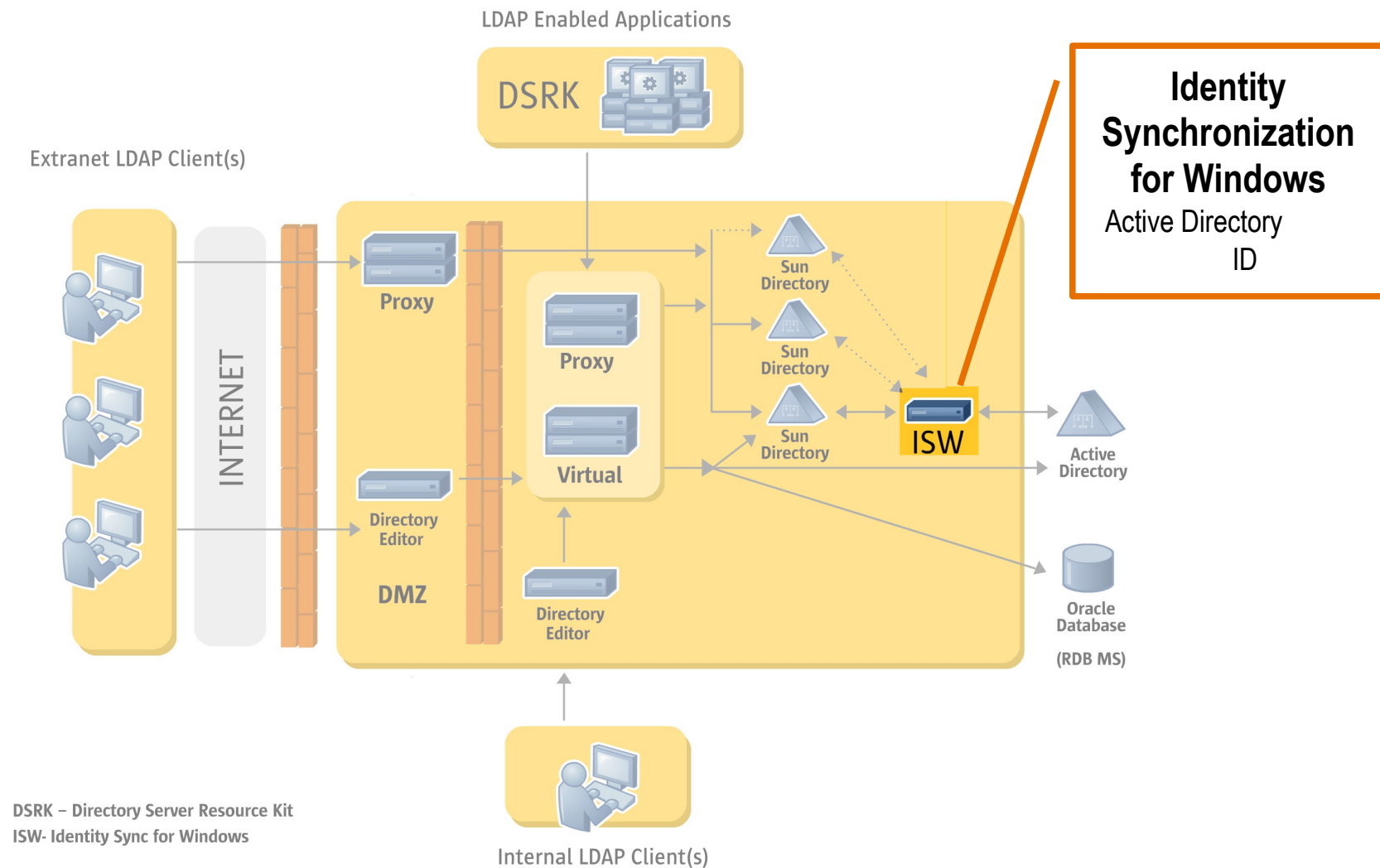
Directory Server 対応プラットフォーム



- Solaris
 - > 10 (SPARC, x86)
 - > 9 (SPARC, x86)
- HP-UX 11.11 (PA-RISC 2.0)
- Red Hat Advanced Server 3.0 U4 (x86), 4.0 U2 (x86)
- Microsoft Windows
 - > 2000 Server SP4
 - > 2000 Advance Server SP4
 - > 2003 Server Standard Edition SP1, Enterprise Edition SP1
- 対応プラットフォームは予告なく変更される可能性があります
- 最新の対応状況については製品ドキュメントをご参照下さい

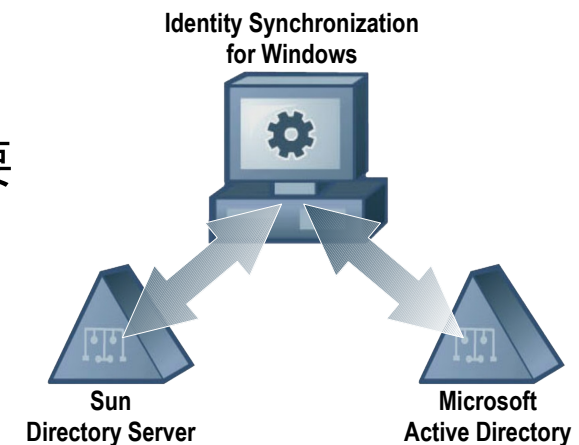
Identity Synchronization for Windows 6.0

Identity Synchronization for Windows



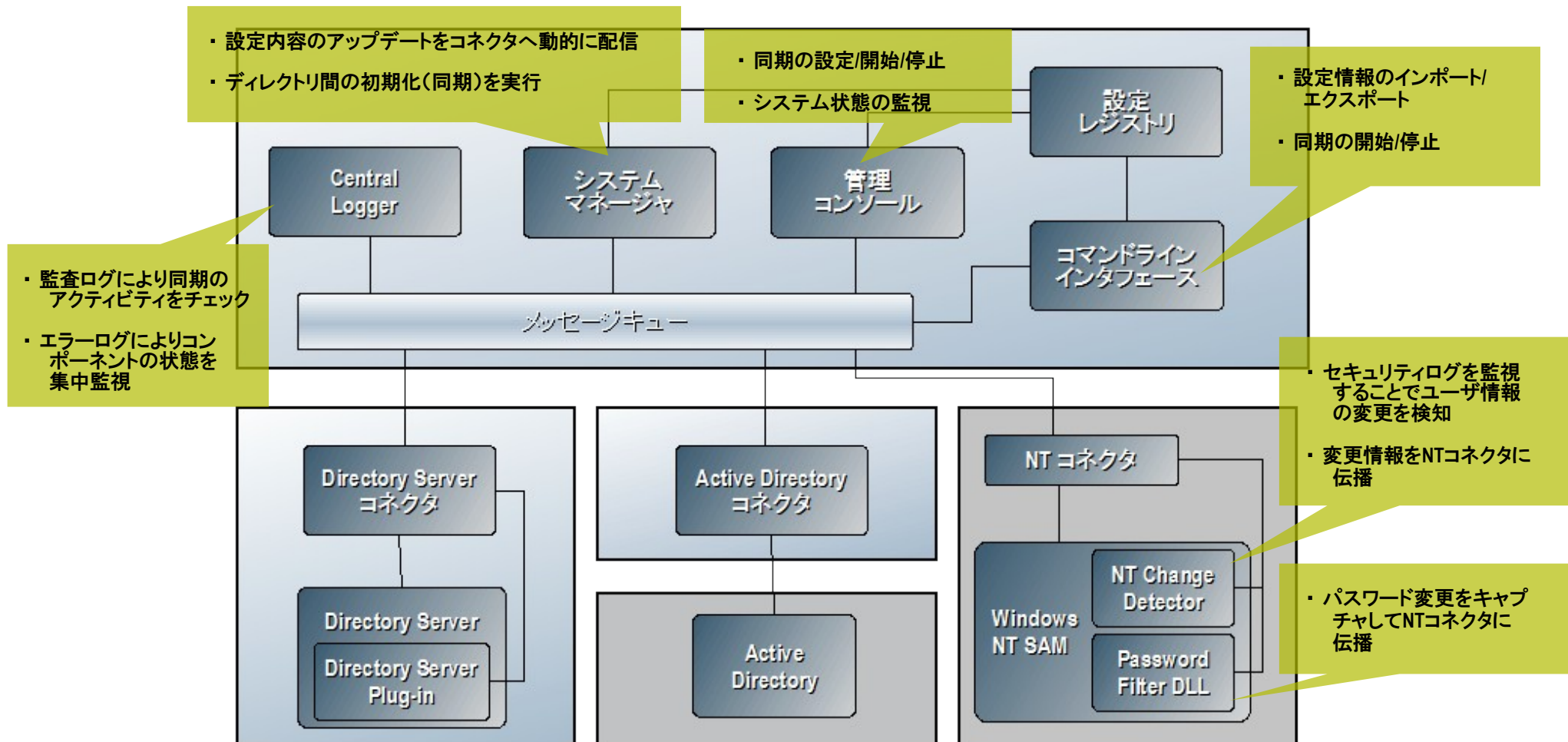
主要機能

- Microsoft Active Directory や Windows NT と Sun Java System Directory Server のアイデンティティ同期を実現
 - > ユーザ作成 / 削除の双方向同期
 - > ユーザ属性の双方向同期
 - ルールにより双方のアカウントをマッピング
 - > ユーザの有効化 / 無効化の同期にも対応
 - > ユーザパスワードの双方向同期
 - Active Directory 側に Plug-in のインストールは不要
 - > グループ (Domain Global Distribution Group, Domain Global Security Group) の同期にも対応
- 同期対象を柔軟に選択可能
 - > 例: 特定の組織配下に属するユーザのみを同期
 - > 例: メールアドレスが同じアカウントを同期
- 属性の動的生成
- ログ・設定情報の集中管理



Identity Synchronization for Windowsのご紹介 アーキテクチャ

- すべてのトラフィックを SSL/3DES で暗号化
- メッセージバスに Message Queue を使用することで高い信頼性を確保



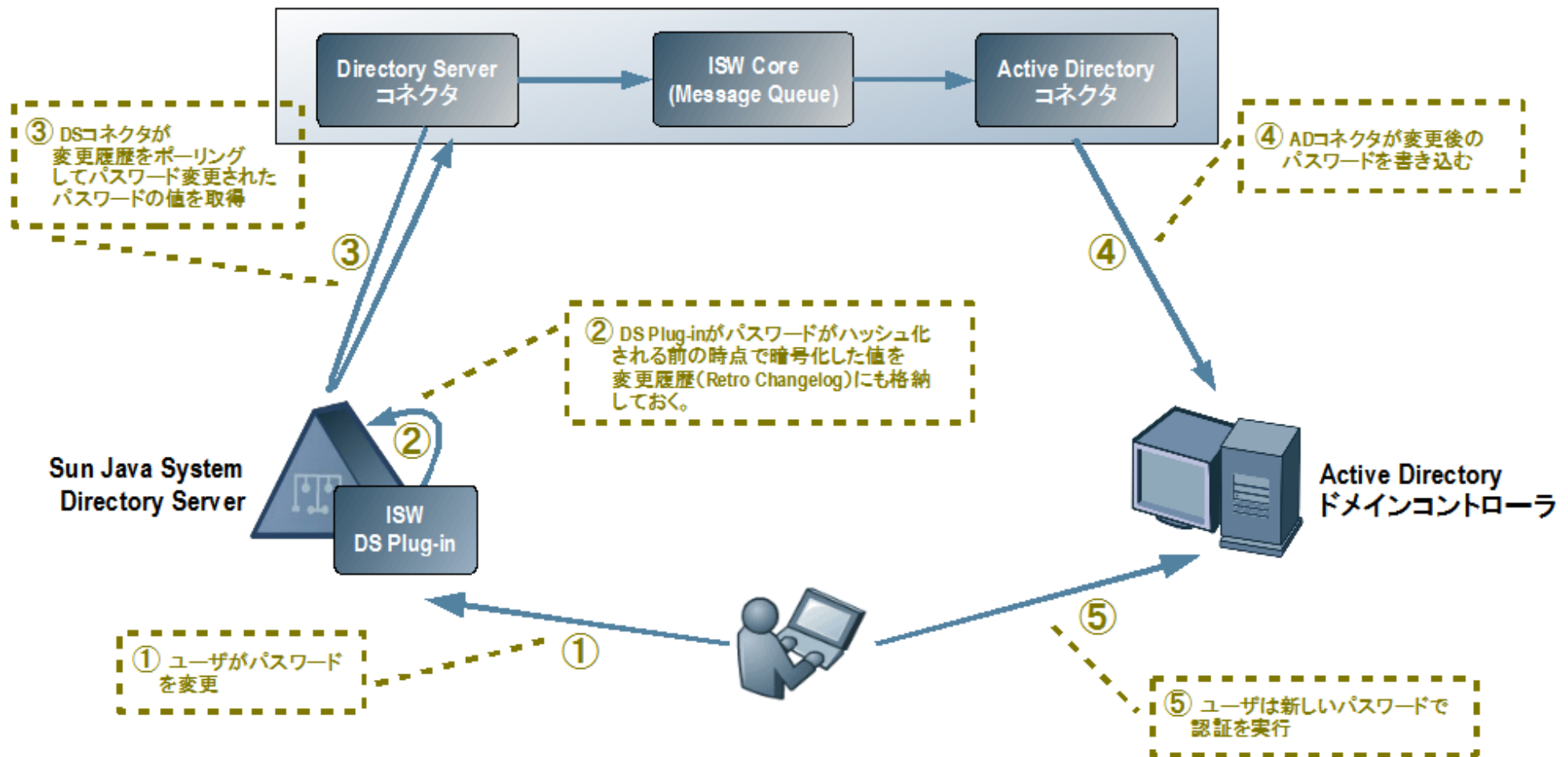
柔軟な同期

- Synchronization User List による同期対象の設定
 - > 特定のツリーのための同期が可能
 - > 特定のユーザのための同期が可能
 - LDAP フィルタによる定義
 - 「に等しい」、「に等しくない」、「または (or)」、「かつ (and)」による条件定義
 - *(アスタリスク)を用いた表現
- アカウント作成時のデフォルト値を動的に作成することも可能
 - > 情報の読み取り元には存在しない属性値を生成
 - 例: cn= % givenname% % sn%
 - 例: homedir=/export/home/% uid%
- アカウントの結びつけルール (UserLinkingOperationList の定義)
 - 例: 「Directory Server の uid と Active Directory の samaccountname が同じ」又は「両ディレクトリ内の givenname と sn の値が等しい」ユーザ
 - Synchronization User List (同期対象の定義)ごとに設定が可能

Identity Synchronization for Windowsのご紹介

Plug-in/変更履歴を使用したパスワード同期

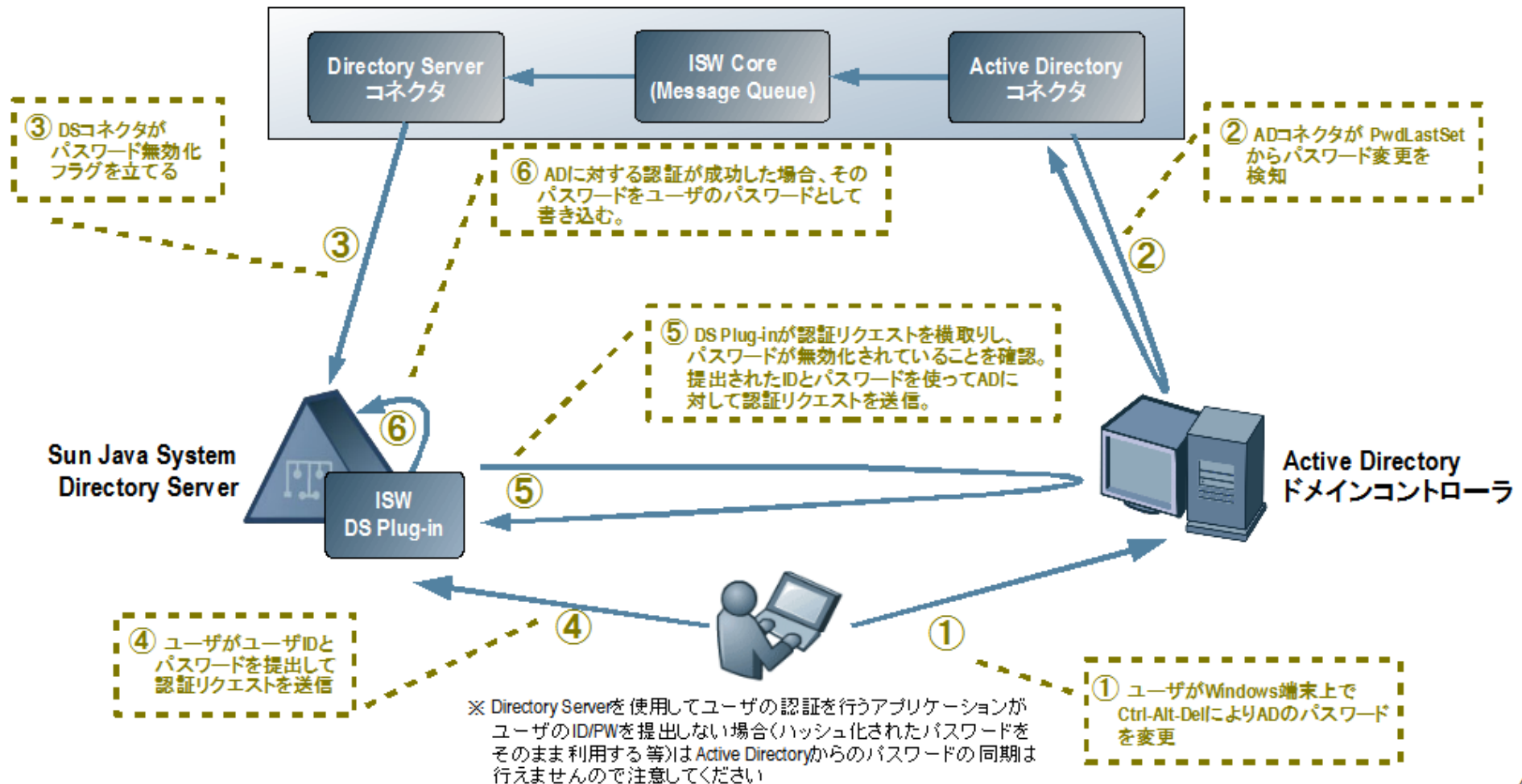
- Directory Server から AD に対するパスワード同期



Identity Synchronization for Windowsのご紹介

On Demand Password Synchronization

- AD から Directory Server に対するパスワード同期



Identity Synchronization for Windowsのご紹介

FAQ

Q1: 複数の Windows ドメイン / NT ドメインやフォレストに対応していますか？

> はい、対応しております

Q2: どの程度の性能を発揮できますか？

> ISW の構成やハードウェアの性能に依存しますが、すべてのコンポーネントを1つのサーバに載せた状態でも (多くの場合) 秒間 10 更新以上を処理することができます

Q3: 対応するデータベースのバージョンはどうなっていますか？

> Windows NT SAM Registry, Active Directory 2000/2003, Directory Server 6 となります

Q4: WAN 経由の同期処理に対応していますか？

> はい、対応しております



Q5: コンピュータオブジェクトの同期に対応していますか？

> 現バージョンでは対応しておりません

Q6: グループの同期に対応していますか？

> はい、対応しております

Q7: 1 対多のアカウント同期に対応していますか？

> Sun Java System Identity Manager をご利用下さい

Q8: Active Directory 同士、Directory Server 同士の同期に対応していますか？

> Sun Java System Identity Manager をご利用下さい

Identity Synchronization for Windowsのご紹介

新機能 及び 対応プラットフォーム

- 新機能 
 - > グループ同期機能
 - > マルチマスタレプリケーションされたレプリカに対するフェイルオーバー対応
 - > RedHat Linux プラットフォーム対応

● 対応プラットフォーム

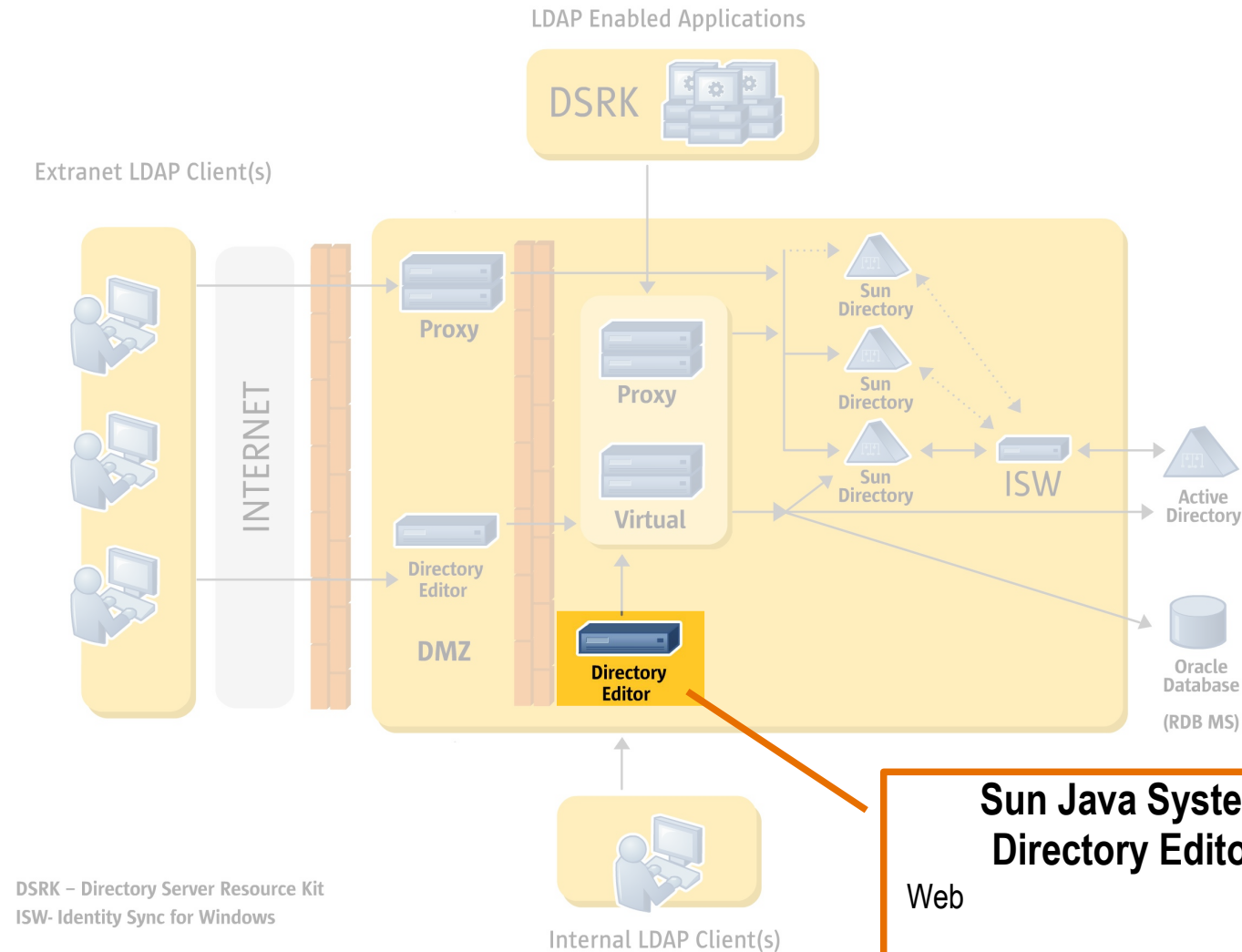
- > Core / コネクタ / Directory Server Plug-in
 - Solaris 8 (SPARC), 9 (SPARC), 10 (SPARC/x86)
 - Red Hat Advanced Server 3.0
 - Microsoft Windows
 - 2000 Server SP4, Advanced Server SP4
 - 2003 Server Standard Edition (最新セキュリティパッチ適用済み状態), Enterprise Edition (最新セキュリティパッチ適用済み状態)
- > Windows NT コネクタ / Plug-in
 - Microsoft Windows NT 4.0 Server SP6a Primary Domain Controller



その他のコンポーネント

Directory Editor のご紹介

Directory Editor



Directory Editorのご紹介

Webベースのエントリ管理ツール

- システム管理者だけでなく組織の管理者やエンドユーザも利用できる Web ベースのディレクトリ管理 / 参照ツール

| バージョン 6.0 |



Copyright ©2006 Sun Microsystems, Inc. All rights reserved. U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements. ご使用は、ライセンス条項に従ってください。この配布には、サードパーティーの開発したソフトウェアが含まれている可能性があります。Sun、Sun Microsystems、サンのロゴマーク、および Java は、米国およびその他の国における Sun Microsystems, Inc. の商標もしくは登録商標です。

Directory Editorのご紹介

主要機能

- ユーザ / グループ / 組織等の管理
- セルフサービス
 - > パスワード変更
 - > あらかじめ設定された参照の可否、変更の可否に基づいてセルフメンテナンス
- 権限委譲
 - > 複数管理者による管理
 - > Directory Server の ACI を利用した組織 / 部署単位の隠蔽等も可能
- 検索機能



参照



人事部の社員ならすべて参照できるが
営業部の社員は自部署しか参照できない

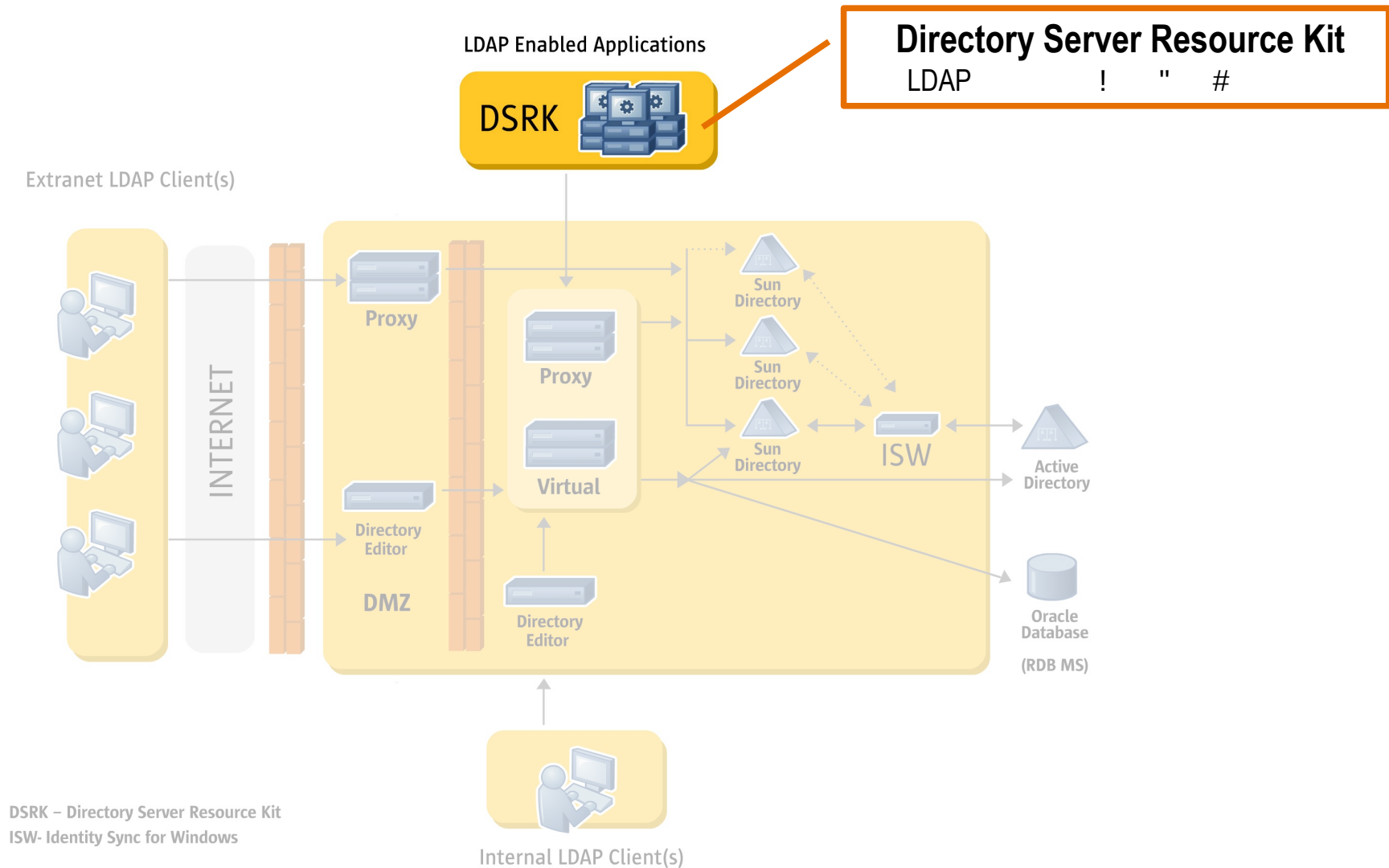


参照



Directory Server Resource Kit のご紹介

Directory Server Resource Kit



Directory Server Resource Kitのご紹介

Directory Server Resource Kit (DSRK) 概要

- Directory Server 対応アプリケーションの開発ツールを提供
- Directory Server を活用するためのツールをバンドル
 - > 性能を測定するためのツール
 - 検索 / 変更 / 認証の性能を測定: searchrate, modrate, authrate
 - テスト用の LDIF ファイル (テストデータ) を作成: makeldif
 - > LDIF ファイルの整形ツール: ldifxform
 - 文字コードの変換、属性名の置換、エントリの並び替え
 - > アクセスログの分析ツール: logconv
 - BIND や検索処理の総計を算出
 - 頻度の高いパラメータを算出 (ランキング)
 - エラーコードのカウント
- サンプルアプリケーションをバンドル
 - > Sun Java System NameFinder



Directory Server Resource Kitのご紹介

Sun Java System NameFinder

Sun Java System NameFinder V5.4 Print | FAQ | Help



→ **NameFinder**

Search for entry

(Press Return to start search.)

[How to search](#)

Name : Taro Yamada

Phone # : 03-1111-2222

FAX # : 03-4444-5555

eMail : Taro.Yamada@Example.COM +

Mobile Phone : 090-7777-8888

Employee Type : Employee

ExampleCorp ID : 123456

Direct Reports : Yoshitake Ohno

Loginname : [tyamada](#)



MySelections (use + to add entries / ☐ Sort entries)

[Company Info](#) | [Feedback](#)

- Java で作られた電子電話帳アプリケーション
- ソースコードレベルで自由にカスタマイズが可能
- 大規模・高負荷に耐え得るアーキテクチャ
 - > Sun Microsystems 社内の標準'電子電話帳'アプリケーションとして数万人の社員が利用

Directory Server Resource Kitのご紹介

対応プラットフォーム



- Solaris
 - > 10 (SPARC, x86)
 - > 9 (SPARC, x86)
- HP-UX 11.11 (PA-RISC 2.0)
- Red Hat Advanced Server 3.0 U4 (x86), 4.0 U2 (x86)
- Microsoft Windows
 - > 2000 Server SP4
 - > 2000 Advance Server SP4
 - > 2003 Server Standard Edition SP1, Enterprise Edition SP1
- 対応プラットフォームは予告なく変更される可能性があります
- 最新の対応状況については製品ドキュメントをご参照下さい

ご参考

ご参考

- 製品概要
 - > Sun Java System Directory Server
 - http://jp.sun.com/products/software/identity/directory_srvr_ee/
- 製品ドキュメント
 - > Directory Server Enterprise Edition 6.0
 - <http://docs.sun.com/app/docs/coll/1224.1>
- 製品ダウンロード
 - > Sun Downloads
 - <http://www.sun.com/download/>
- Developer Forums
 - > Sun Java System Directory Server
 - <http://forum.java.sun.com/forum.jspa?forumID=761>



Sun Java System Directory Server Enterprise Edition 6 Overview

Sun Microsystems K.K.
Sun Java Software Practice.

