OpenLDAPの syncreplレプリケーション

OSC 2007 Hokkaido

日本LDAPユーザ会／NECソフトウェア北海道

稲地 稔

日本LDAPユーザ会について

2007年4月1日に正式発足

- 目的
  - LDAPに関する情報交換
    - 技術情報、イベント情報、人的交流
  - LDAP利用の普及促進

- 活動内容
  - Webによる情報発信
    - *http://www.ldap.jp/*
  - メーリングリストによる情報交換
  - 技術セミナー、OSC 、 LWCのようなイベントに参加

講師紹介

- 稲地 稔(いなち みのる)
  - NECソフトウェア北海道　社員
  - 日本LDAPユーザ会スタッフ

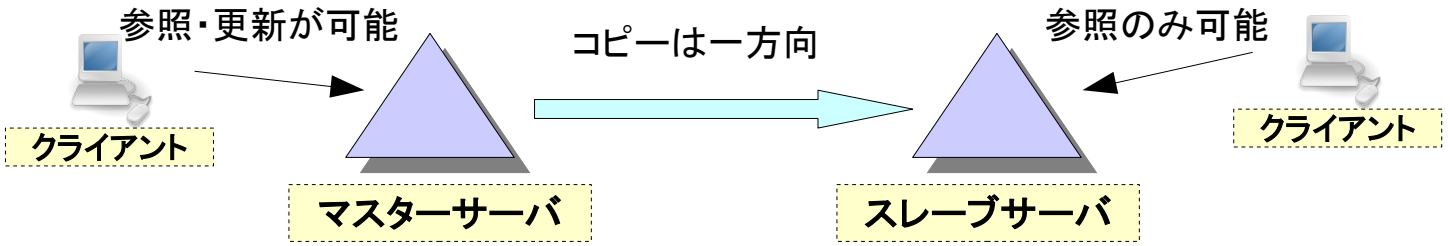
- OpenLDAPドキュメントの翻訳
  - *http://www5f.biglobe.ne.jp/~inachi/openldap/*

- 著作
  - 2001年10月 技術評論社 WEB+DB Press Vol.5
    - 特集2　社内システム増強計画
第1章「OpenLDAPとPHPによる高速検索 社員情報管理システムの作り方」
  - 2003年8月 技術評論社「OpenLDAP入門」
  - 2006年5月 技術評論社 LDAP Super Expert
    - 特集1 OpenLDAP 2.3の強化ポイント

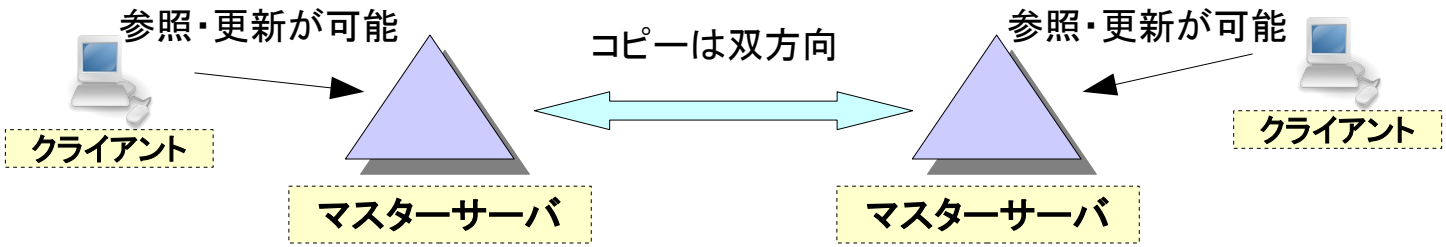
ディレクトリサービスのレプリケーション

- ディレクトリサーバのデータを他サーバに自動コピーする機構
- 高可用性、信頼性、負荷分散のために必要
- 構成方法：シングルマスターとマルチマスター

シングルマスターレプリケーション



マルチマスターレプリケーション



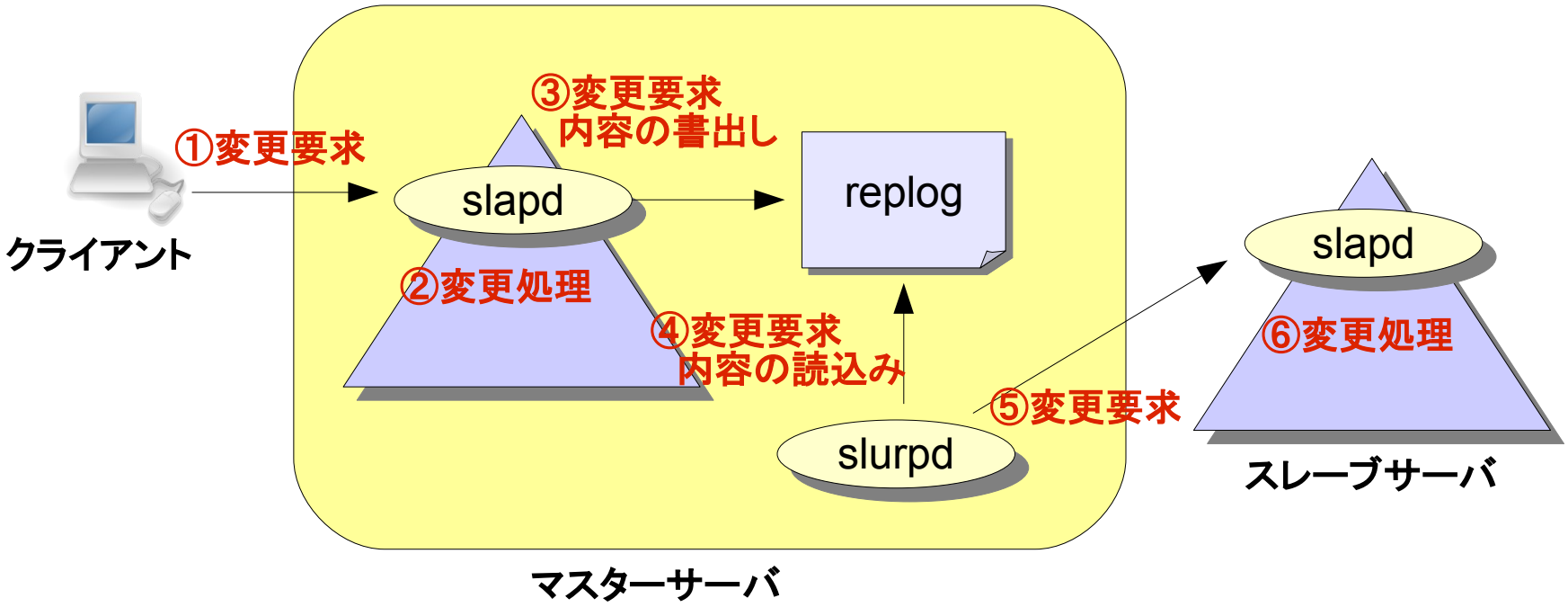
OpenLDAPのレプリケーション

■ 2種類の異なるレプリケーション方式を提供
■ 両者ともシングルマスターレプリケーション

- slurpd方式
  - ミシガン大学のLDAP処理系から引き継いだ伝統的な方式
  - 長い実績（多くの情報、枯れた実装）
  - 開発は停滞状態
- syncrepl方式
  - バージョン2.2よりサポートされた、まだ若い方式
  - 少ない実績（情報が不足）
  - 活発な開発

slurpd方式のレプリケーション

■変更操作の履歴を元に複製
■マスターからスレーブへのPush
■ステートレス（相手の状態を関知しない）



slurpd方式の問題

syncrepl登場の背景にはslurpdの運用上の問題

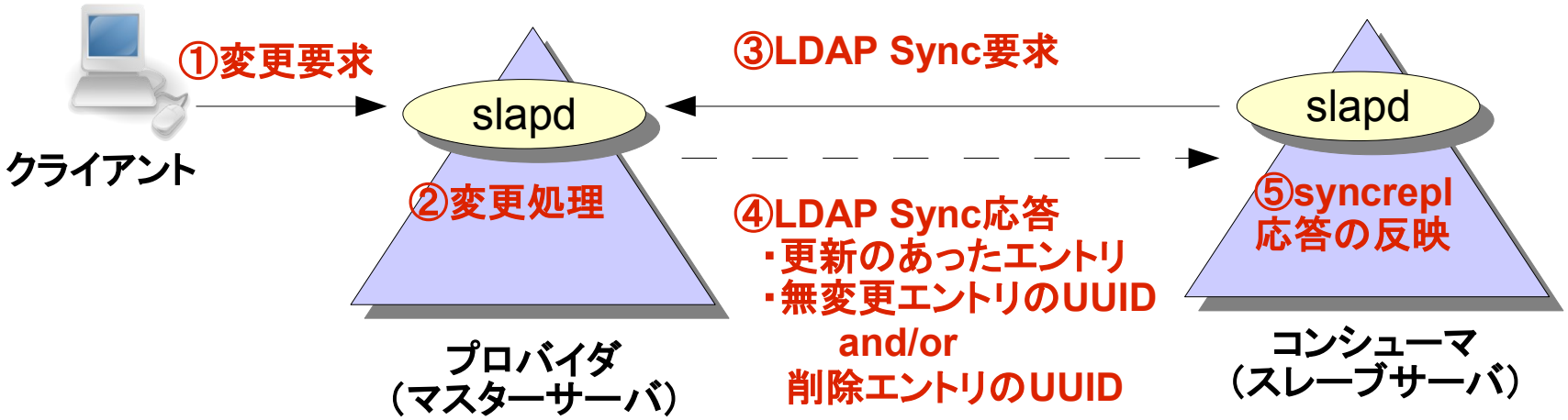
- スレーブの追加時に、マスターDBのコピーが必要
  →マスターサーバを停止しなければならない

- スレーブの状態に関知せず更新操作を再現
  →エラー発生時に不整合が発生する可能性
  →管理者が手作業で修正するか、マスターDBのコピーをやり直し

そして、ついに・・・

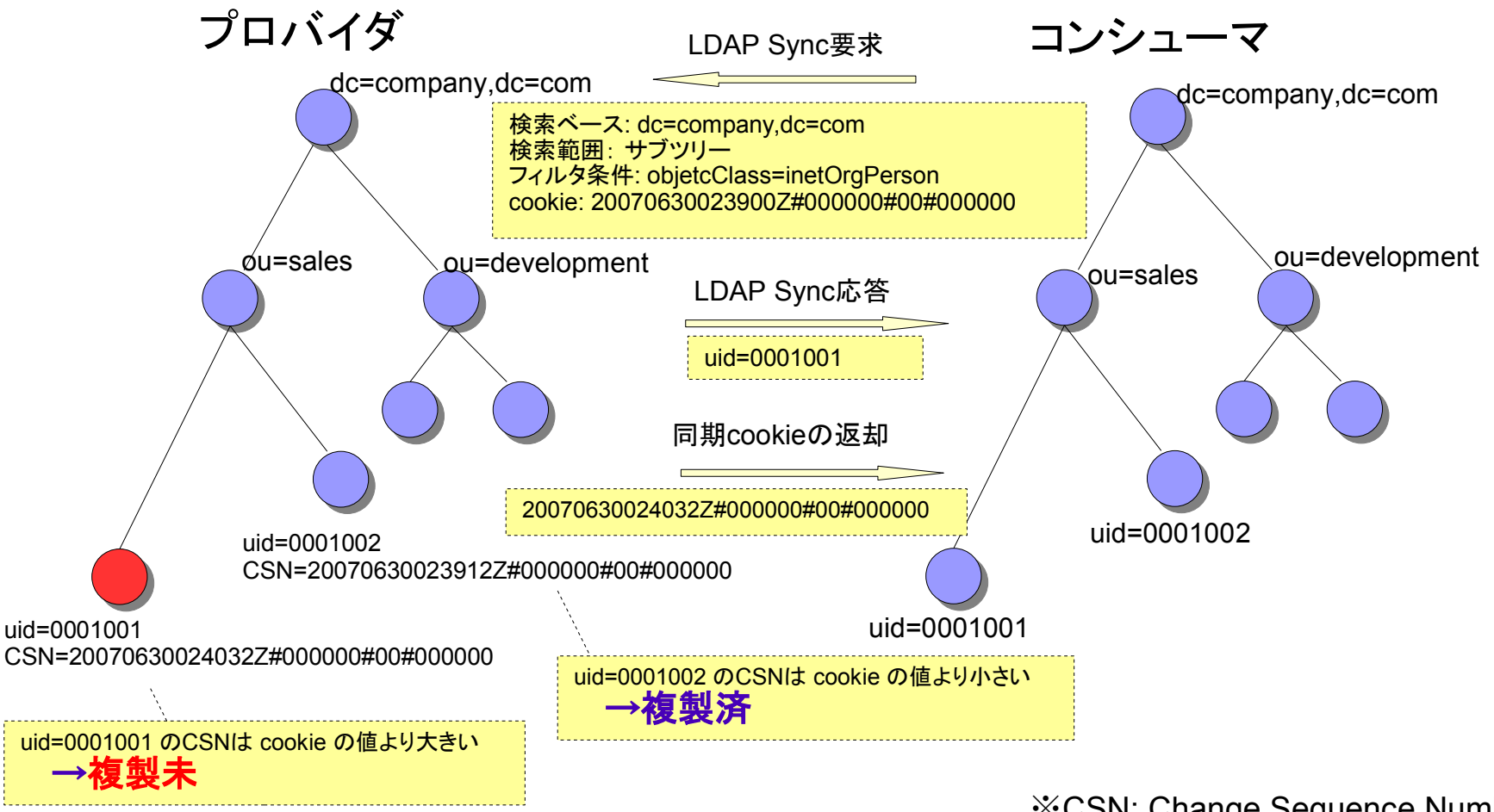
syncrepl方式のレプリケーション

■拡張した検索操作(LDAP Sync)による複製
■コンシューマ(スレーブ)からプロバイダ(マスター)をPull
■ステートフル(相手の状態を反映)



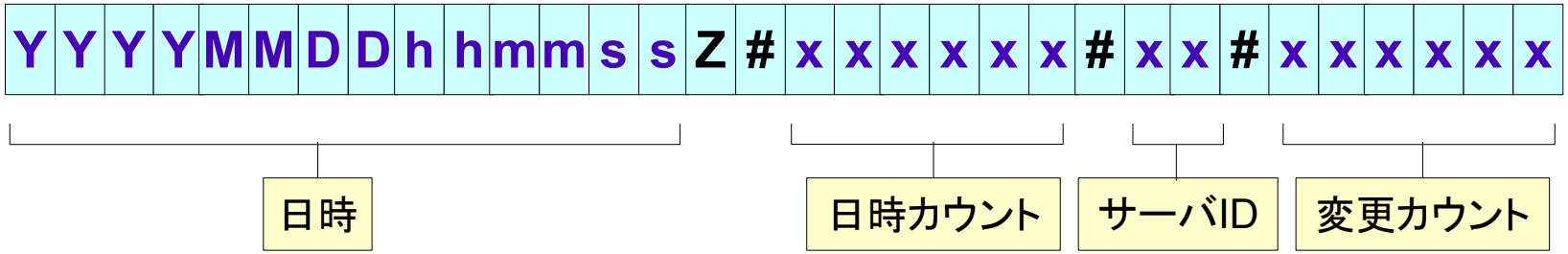
LDAP Sync操作の基本

通常の検索条件 ＋ cookie で複製するエントリを選別



※CSN: Change Sequence Number

CSN（Change Sequence Number）



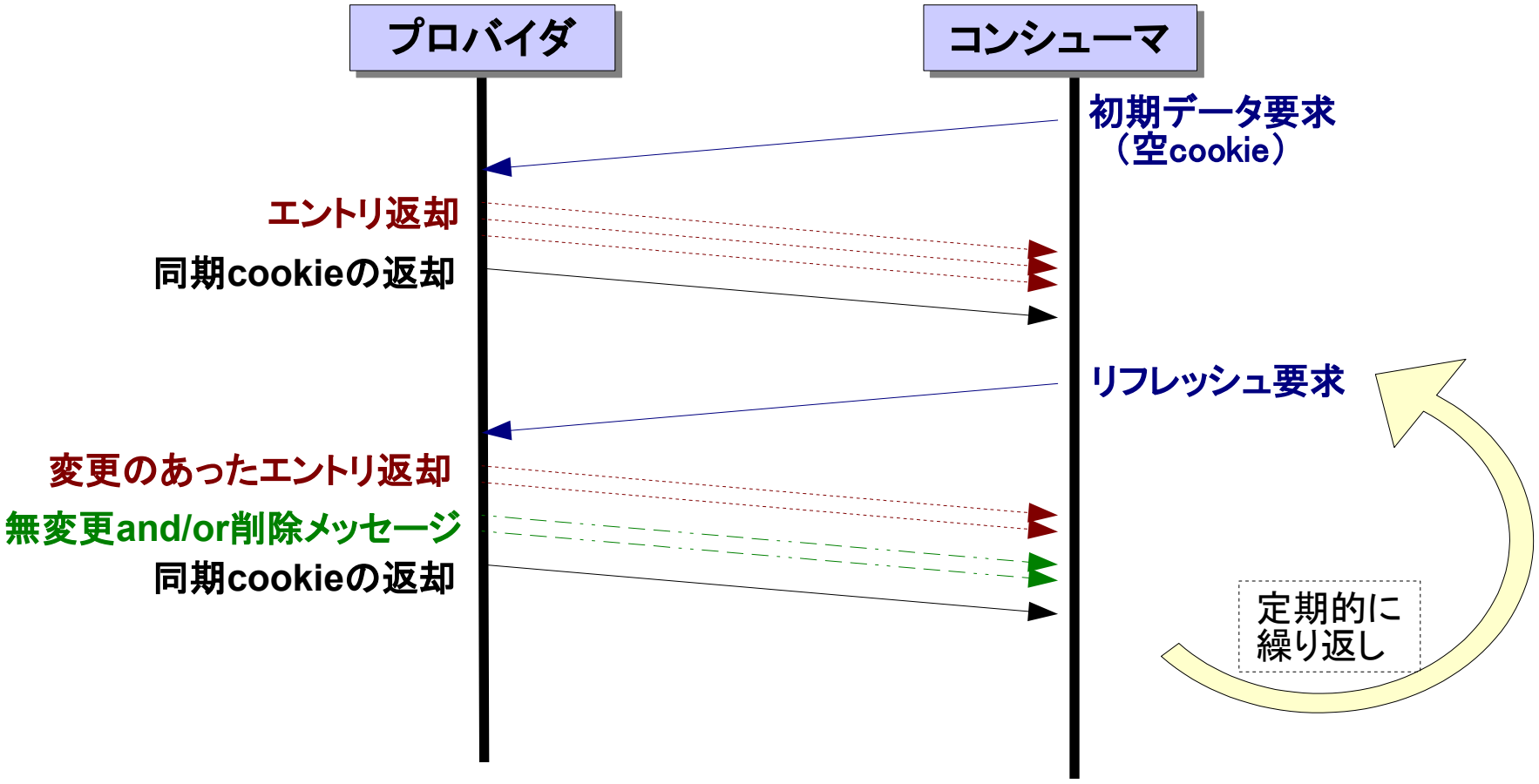
- **日時**
  変更のあった日時（標準時、年月日時分秒）
- **日時カウント**
  同一日時での変更順（16進数6桁）
- **サーバID**
  変更したサーバのID（16進数2桁、未使用）
- **変更カウント**
  同一操作での変更順（16進数6桁、未使用）

syncreplで利用する運用属性

- entryCSN
  エントリの変更時に更新されるCSN
- contextCSN
  データベースで管理する最大のCSN
- entryUUID
  エントリを一意に識別するためのUUID
  （Universal Unique IDentifier）
  →無変更、削除エントリの通知に利用
  （DNは変更できるので一意なIDとして使えない）

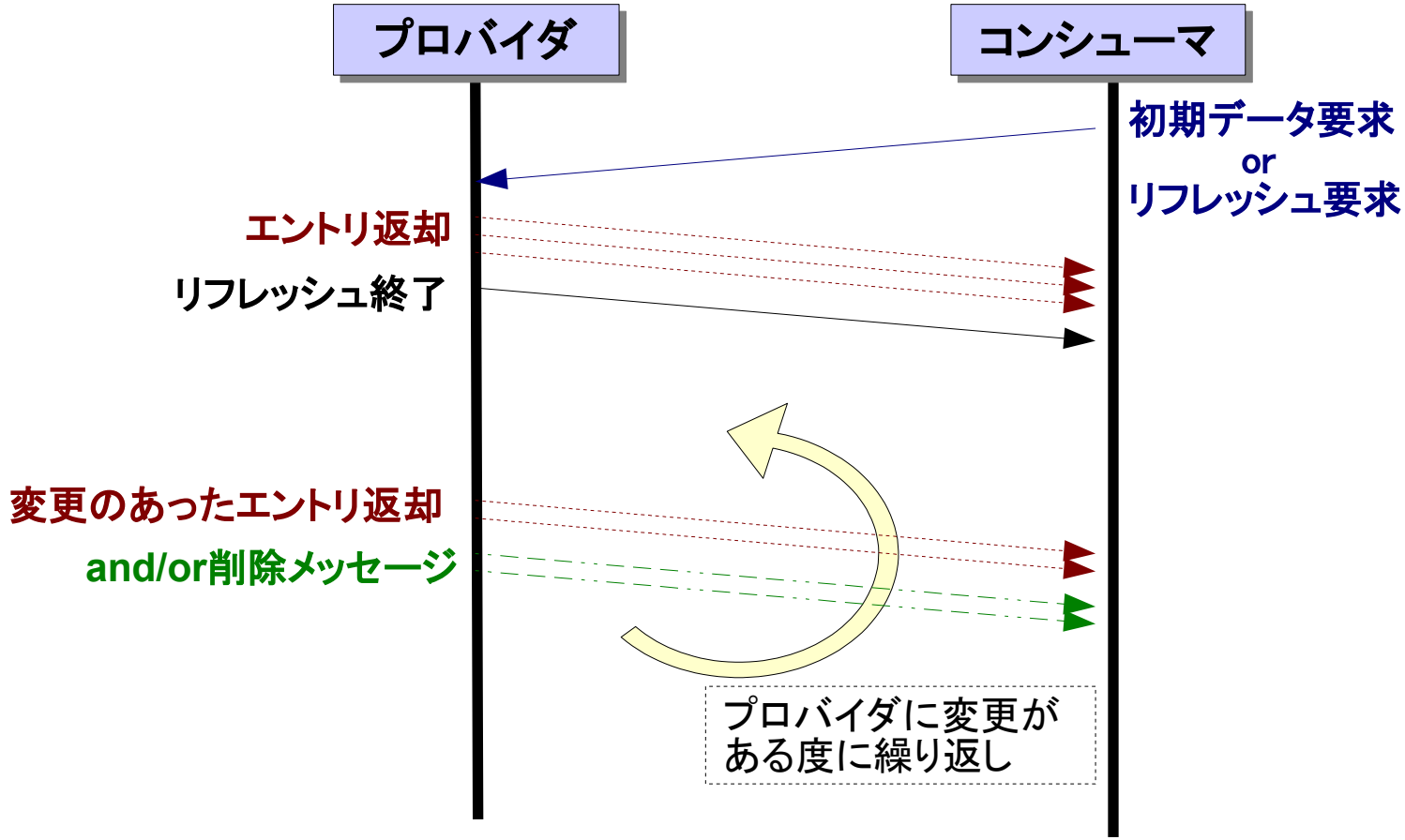
refreshOnlyモード

プロバイダへの定期的な接続・LDAP Sync操作の実行



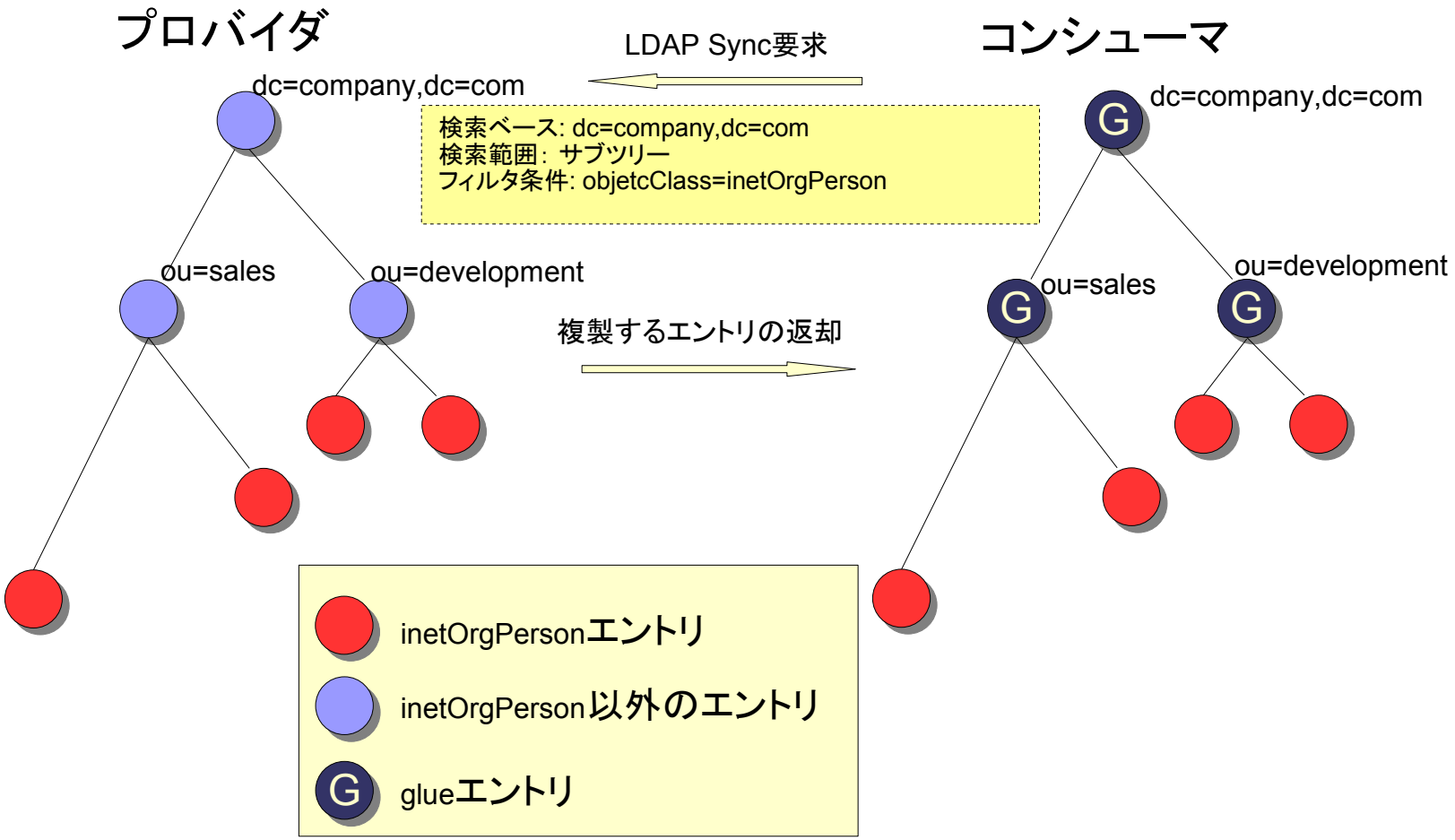
refreshAndPersistモード

コンシューマが停止するまでLDAP Sync操作が継続



glueエントリ

- syncreplで複製されないエントリを補完
- 通常のLDAP操作では不可視



設定…プロバイダ側

- データベース設定にsyncprovオーバレイを指定
- 必要に応じてsyncprov固有のディレクティブを指定

syncprovオーバレイ固有の設定ディレクティブ

ディレクティブ	説明
syncprov-checkpoint	データベースにcontextCSNを実際に書き込む間隔を指定 デフォルトではサーバ終了までデータベースに書き込まない
syncprov-sessionlog	セッションログに保持できる操作の数を指定 デフォルトでは記録しない
syncprov-nopresent	無変更エントリの通知が不要かをTRUE/FALSEで指定 デフォルトはFALSE
syncprov-reloadhint	cookieが空、あるいは古いときにすべてのエントリを再送するかのフラグを見るかをTRUE/FALSEで指定 デフォルトはFALSE

設定例…プロバイダ側

```
# オーバレイをモジュール化している場合はロードが必要
modulepath /usr/local/libexec/openldap
moduleload syncprov.la
    ...

# データベース設定の開始
database bdb
suffix dc=company,dc=com
    ...

# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID eq

# syncprovオーバレイの利用を指定
overlay syncprov

# セッションログの利用を指定(100操作分)
syncprov-sessionlog 100
```

設定…コンシューマ側

- データベース設定にsyncreplディレクティブを指定
- 接続情報＋認証情報＋モード＋検索条件＋α

syncreplディレクティブのパラメータ

パラメータ	説明
rid	プロバイダから見て一意なIDを3桁の10進数で指定
provider	プロバイダをLDAP URIで指定
type	refreshOnlyかrefreshAndPersistかを指定
interval	refreshOnlyの場合の実行間隔を指定(DD:hh:mm:ss)
retry	プロバイダに接続できない場合の再トライ間隔を指定
searchbase	検索ベース
filter	検索フィルタ
scope	検索スコープ
attrs	取得する属性

設定…コンシューマ側(２)

syncreplディレクティブのパラメータ(続き)

パラメータ	説明
attrsonly	属性型だけの取得
sizelimit	取得するエントリ数の制限(デフォルト無制限)
timelimit	検索の時間制限(デフォルト無制限)
schemachecking	スキーマのチェックをするかをon/offで指定
starttls	startTLS拡張操作により通信路を保護する(yesまたはcritical)
bindmethod	バインド方式をsimpleかsaslのどちらかで指定
binddn	simpleバインドの場合のDNを指定
saslmech	SASL認証の認証機構を指定
authcid	SASL認証の認証IDを指定
authzid	SASL認証の認可IDを指定
credentials	認証パスワードを指定
realm	SASL認証のレルムを指定
secprops	SASL認証のセキュリティプロパティを指定

設定例･･･コンシューマ側

```
# データベース設定の開始
database bdb
    ...
# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID eq

# コンシューマの設定(3分間隔でレプリケーションを実行)
syncrepl rid=1
        provider=ldap://main.company.com
        type=refreshOnly
        interval=00:00:03:00
        searchbase="dc=company,dc=com"
        filter="(objectClass=inetOrgPerson)"
        scope=sub
        attrs="*"
        schemachecking=off
        bindmethod=simple
        binddn="cn=syncuser,dc=company,dc=com"
        credentials=secret
```

syncreplに問題はないのか

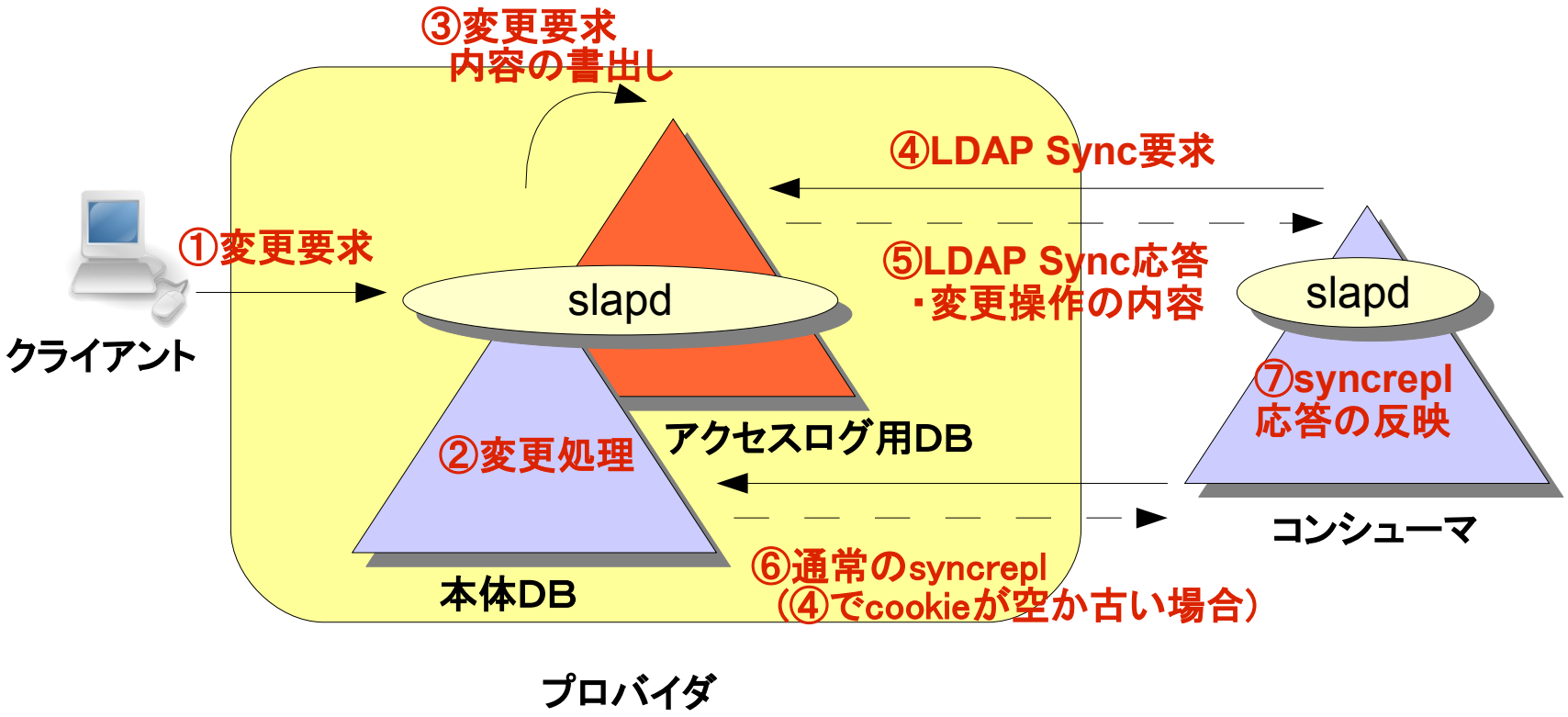
■ syncreplにも問題が無いわけではない
■ 多くの問題には回避策または将来的に解決する目処あり

- 更新差分レプリケーションができない
  - 小さな更新でもエントリの全内容が対象→大量の更新では帯域に負荷
- Push型のレプリケーションができない
  - スレーブ側からのアクセスを禁止しているFireWallがある場合にはsyncreplの適用が困難
- 他LDAPサーバ製品にレプリケーションできない
  - LDAP Sync操作のサポートは(現在のところ)OpenLDAPのみ
- 相変わらずマルチマスター構成にできない
- 厳密な意味での同期レプリケーションモードが無い

syncreplの応用
delta-syncreplとPush型syncrepl

delta-syncrepl

- 変更履歴を元にしたsyncreplを実現
- 変更履歴の記録にアクセスログを利用
- 初期ロード、cookieが古い場合は通常のsyncreplを実行



設定…プロバイダ側(アクセスログ用DB)

- アクセスログ用DBにもsyncprovオーバレイを適用
- syncprov-nopresentとsyncprov-reloadhintの指定が必須

```
# アクセスログ用データベース設定の開始
database bdb
suffix cn=accesslog
    ...

index objectClass,reqStart,reqResult   eq
# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID  eq

# syncprovオーバレイの利用を指定
overlay syncprov

# 無変更エントリを返さない
syncprov-nopresent TRUE

# LDAP Sync要求のreloadhintフラグを無視しない
syncprov-reloadhint TRUE
```

変更操作の内容を通知できればいいので、無変更エントリの通知は不要

cookieが空や古くても全ロードが起きないように

設定…プロバイダ側（本体DB）

- 通常のsyncreplと同様にsyncprovオーバレイを適用
- アクセスログの記録のためにaccesslogオーバレイを適用
- 成功した変更操作だけをアクセスログに記録するよう設定

accesslogオーバレイ固有の設定ディレクティブ

ディレクティブ	説明
logdb	記録するデータベースをsuffixで指定
logops	記録する操作の種別を指定 変更操作だけを記録するには“write”を指定
logold	変更前の情報を記録するエントリを検索フィルタで指定 delta-syncreplでは指定の必要なし
logsucess	成功した操作だけを記録するかをTRUE/FALSEで指定 delta-syncreplではTRUEを指定
logpurge	記録の保持期間と、保持期間を超えたエントリを調査する間隔を指定

設定例…プロバイダ側（本体DB）

```
# データベース設定の開始
database bdb
suffix dc=company,dc=com
    ...
# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID eq

# syncprovオーバレイの利用を指定
overlay syncprov

# アクセスログオーバレイの指定
overlay accesslog

#アクセスログ用のデータベースを指定
logdb cn=accesslog

# 変更操作だけをアクセスログに記録
logops write

# 成功した操作だけをアクセスログに記録
logsuccess TRUE

# アクセスログDBを毎日スキャンし、３日経ったエントリを除去
logpurge 03+00:00 01+00:00
```

設定…コンシューマ側

通常のsyncreplの設定に加え、logbase, logfilter, syncdataを指定

```
# データベース設定の開始
database bdb
    ...
# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID eq

# コンシューマの設定(3分間隔でレプリケーションを実行)
syncrepl rid=1
        provider=ldap://main.company.com
        type=refreshOnly
        interval=00:00:03:00
        searchbase="dc=company,dc=com"
        filter="(objectClass=inetOrgPerson)"
        scope=sub
        attrs="*"
        schemachecking=off
        bindmethod=simple
        binddn="cn=syncuser,dc=company,dc=com"
        credentials=secret
        logbase="cn=accesslog"
        logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
        syncdata=accesslog
```

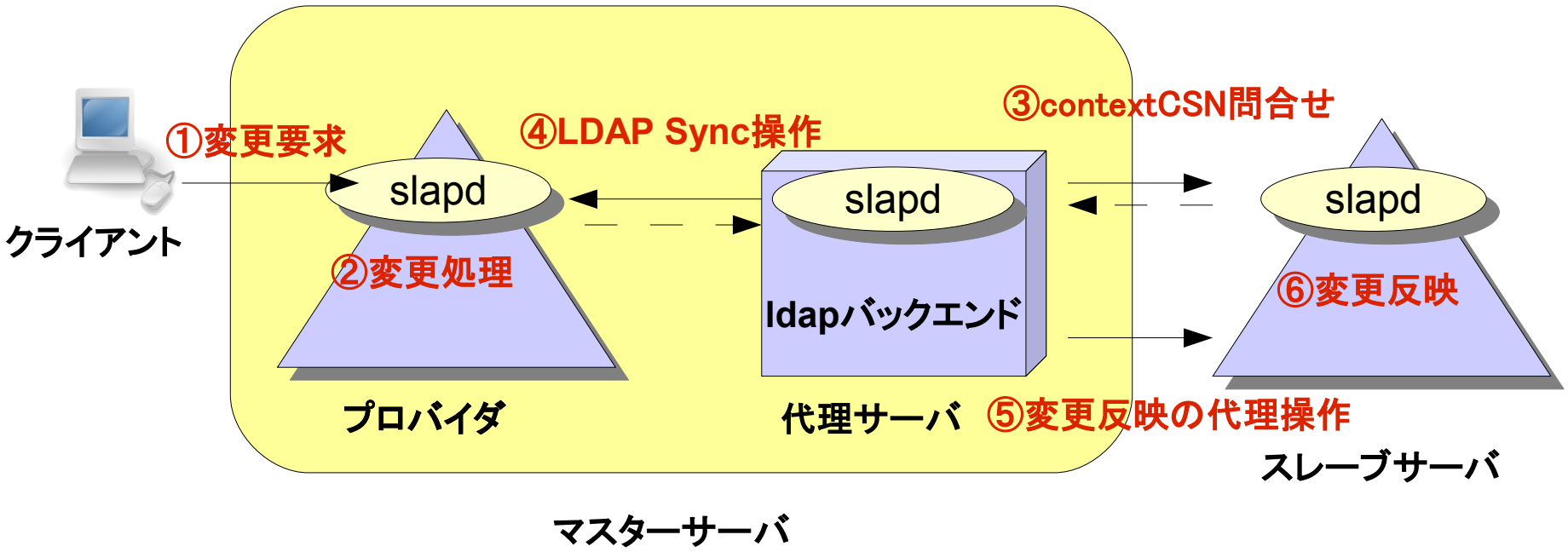
アクセスログにLDAP Sync要求する際の検索ベース

アクセスログにLDAP Sync要求する際の検索フィルタ

Delta-syncreplのアクセス情報がアクセスログであることを示す

Push型syncrepl

- syncreplでpush型のレプリケーションを実現
- ldapバックエンドとsyncreplを組み合わせた代理サーバを用意
- slurpdからの置き換えに有効
- 他LDAP製品へレプリケーションできる可能性も



設定例・・・プロバイダ側

通常のプロバイダ設定と同様

```
# データベース設定の開始
database bdb
suffix dc=company,dc=com
    ...

# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID eq

# syncprovオーバレイの利用を指定
overlay syncprov

# セッションログの利用を指定(100操作分)
syncprov-sessionlog 100
```

設定例・・・スレーブ側

- slurpd方式の場合のスレーブと同様の定義
- 加えて、更新を許可するDNのためのデータベース定義

```
# データベース設定の開始
database bdb
suffix dc=company,dc=com
    ...

# syncreplで利用する運用属性にインデックスをつける
index entryCSN,entryUUID eq

# 更新を許すDNを指定
updatedn “cn=Monitor”
    ...

# 更新を許すDNのための便宜的なデータベース定義
database monitor
rootdn “cn=Monitor”
rootpw monitor
```

データベースが空でもレプリケーション可能とするために、他DBの管理者用DNを利用

設定・・・代理LDAPサーバ

- ldapバックエンドデータベースにsyncreplを指定
- 代理アクセス先にスレーブサーバを指定

```
# ldapバックエンドデータベース設定の開始
database ldap
suffix dc=company,dc=com
  ...
# 代理アクセス先にスレーブサーバを設定
uri ldap://slave.company.com

# スレーブサーバへのレプリケーションのための認証情報
acl-bind bindmethod=simple  binddn="cn=Monitor"  credentials=monitor

# コンシューマの設定(3分間隔でレプリケーションを実行)
syncrepl rid=1
        provider=ldap://main.company.com
        type=refreshOnly
        interval=00:00:03:00
        searchbase="dc=company,dc=com"
        filter="(objectClass=inetOrgPerson)"
        scope=sub
        attrs="*"
        schemachecking=off
        bindmethod=simple
        binddn="cn=syncuser,dc=company,dc=com"
        credentials=secret
```

バージョン2.4での syncrepl強化項目

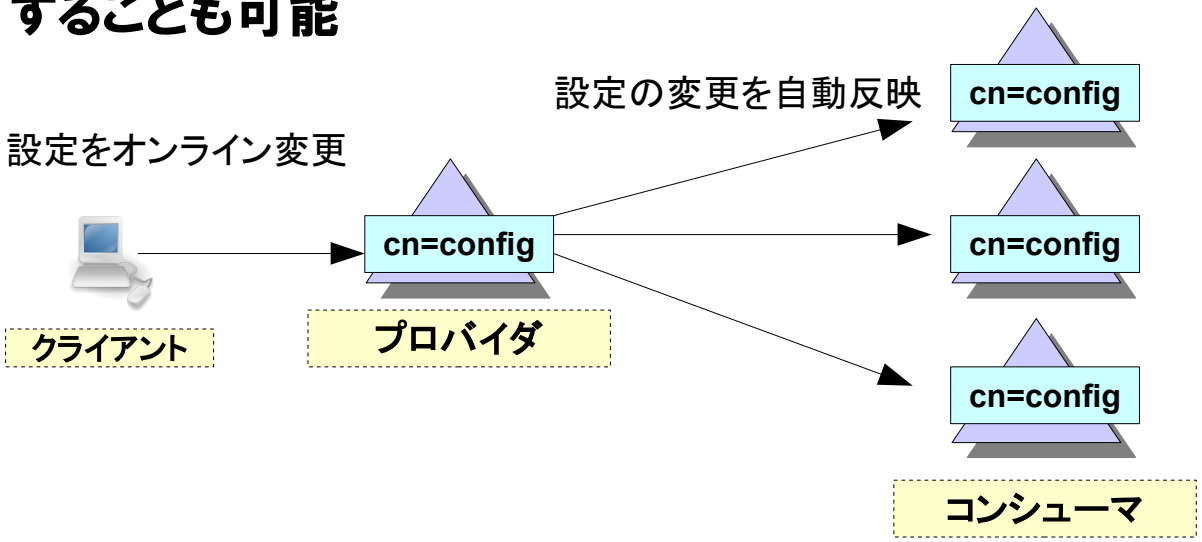
■注意■

CVS上の最新開発版ソースを元にした調査であるため
実際のリリース版とは異なる場合があります

設定データベースのレプリケーション

■ syncprovオーバレイ、syncreplディレクティブの指定が可能に

- より管理が容易になる可能性
  - プロバイダの設定をオンラインで更新、コンシューマへの自動反映
  - スキーマの変更もレプリケーション可能
  - 検索条件によりプロバイダ固有の設定をレプリケーションされないようにすることも可能



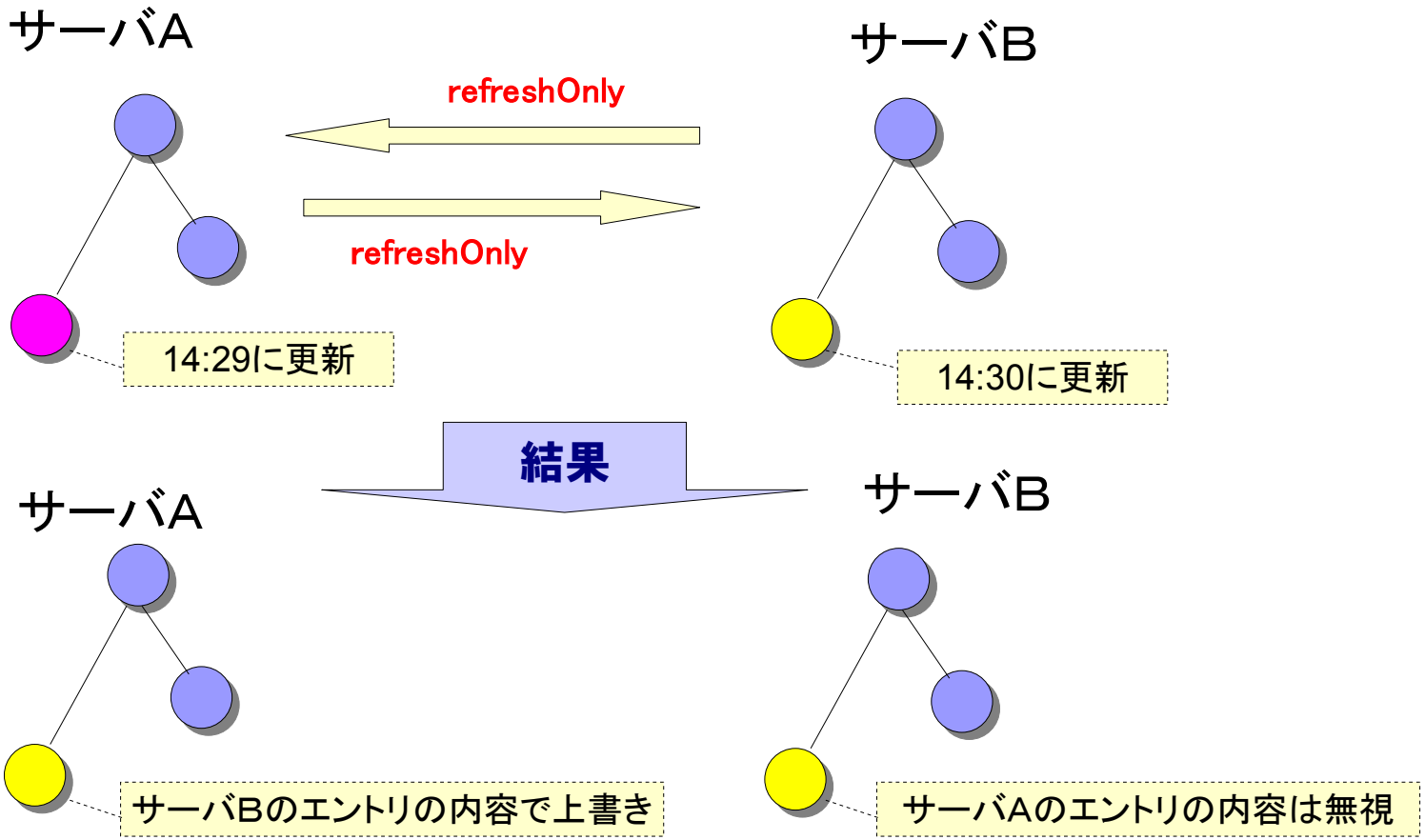
マルチマスターレプリケーション

■ 構成サーバのすべてがプロバイダ＆コンシューマ
■ 構成するサーバ間で一意なIDを各サーバに設定
■ mirrormodeディレクティブによりすべてのサーバが更新可能

- 1データベースに複数のsyncrepl指定が可能
  - N-Wayマルチマスター構成が可能
- エントリレベルの衝突解決
  - 属性レベルの衝突の判定は不可
- CSNのフォーマットが変更
  - 日時がマイクロ秒単位に → 衝突判定の精度向上
  - サーバIDが16進数3桁に → 更新したサーバのIDを記録
- delta-syncreplのマルチマスター化は不可
  - 2.4系列の後のほうで可能となる予定

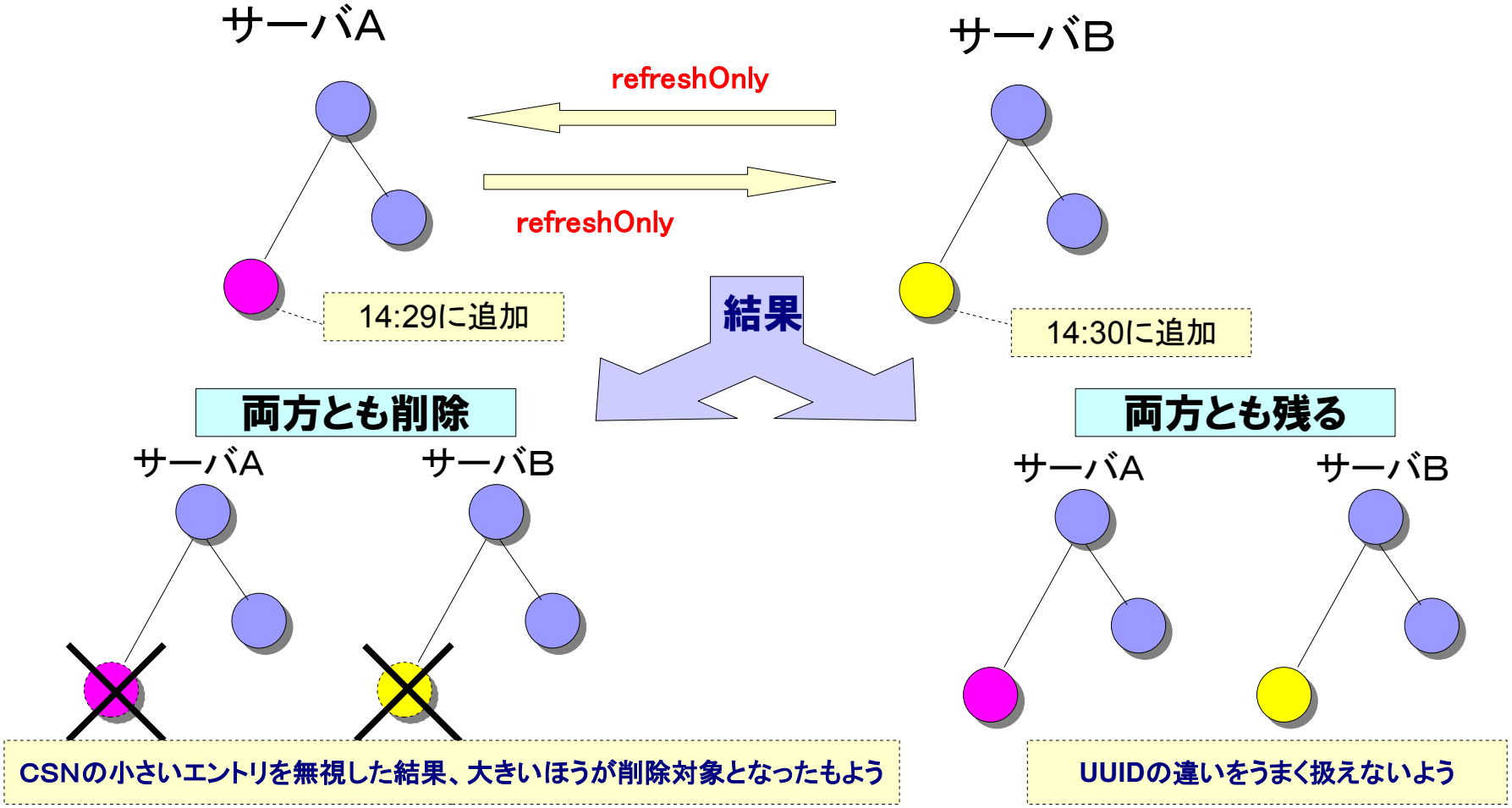
エントリ更新の衝突の解決

- refreshOnlyモードの実行間に異サーバで同一エントリを更新
- CSNの大きい方を優先して解決



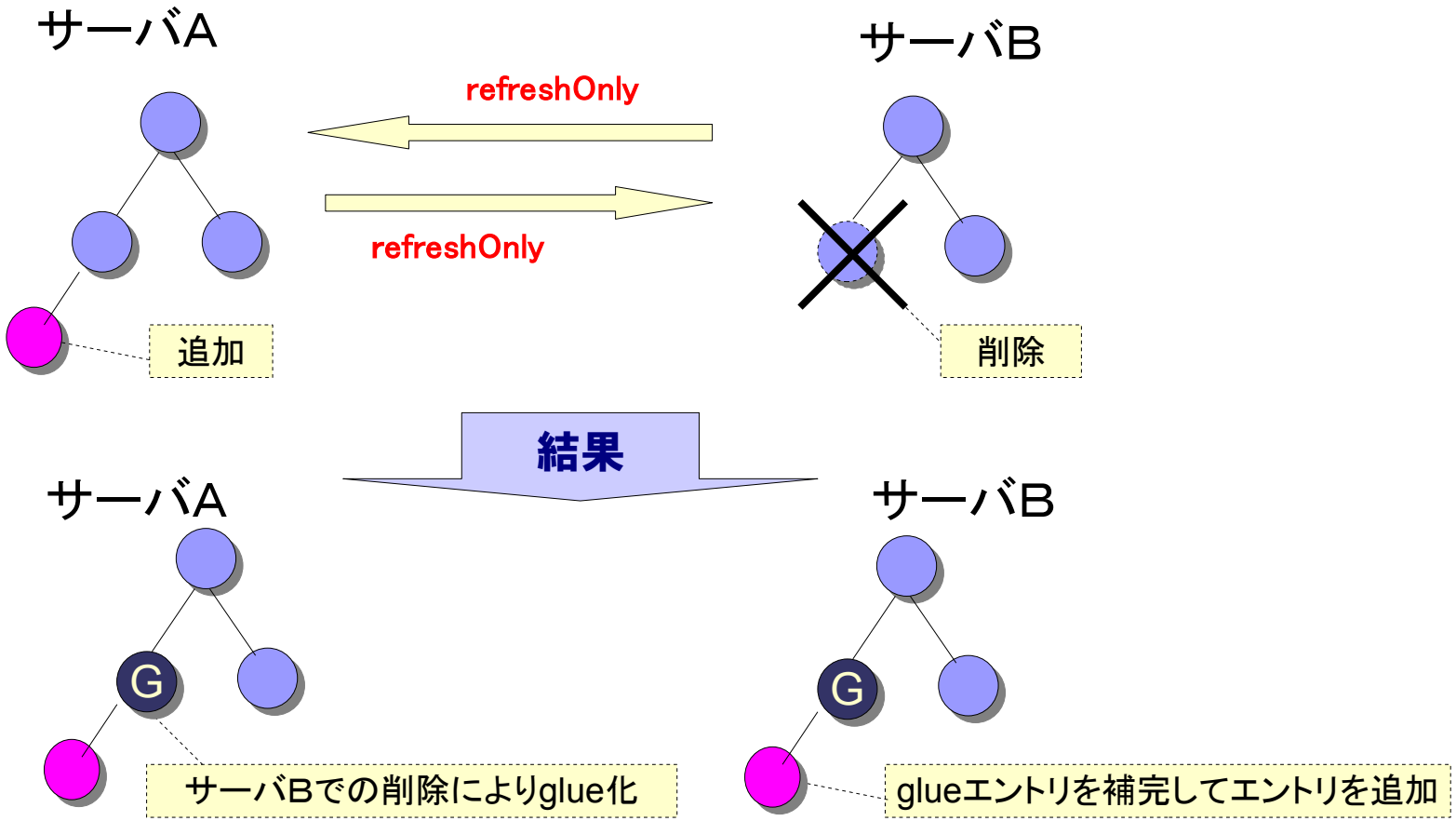
エントリ追加の衝突の解決

- refreshOnlyモード実行間に異サーバで同一DNのエントリを追加
- CSNの大きい方を優先しようとしているが、うまくいっていない



親子関係の衝突の解決

- refreshOnlyモードの実行間に異サーバで同一エントリを更新
- CSNの大きい方を優先して解決



まとめ

- バージョン2.4からはレプリケーションにsyncreplが必須
  - slurpdは消滅
- syncreplは検索操作を拡張したPullベースのレプリケーション
  - 検索対象とならないエントリはglueエントリで補完
- 従来のslurpdの利点もほぼ包括可能に
  - delta-syncrepl
  - Push型syncrepl
- バージョン2.4からは設定データベースとN-Wayマルチマスタ構成のレプリケーションも可能

ご静聴ありがとうございました