

# WSRFに基づく情報サービスの XACMLによるアクセス制御

竹房あつ子<sup>1</sup>, 中田秀基<sup>1</sup>, 柳田誠也<sup>1,2</sup>,  
工藤知宏<sup>1</sup>, 田中良夫<sup>1</sup>, 関口智嗣<sup>1</sup>

<sup>1</sup>産業技術総合研究所グリッド研究センター  
<sup>2</sup>数理技研

# グリッドにおける情報サービス

- グリッドでは, 広域に分散する資源を利用
    - 計算機やネットワーク等の状態やジョブの実行状況の監視要求
    - SSH等で資源に直接ログインして取得可能だが, 監視すべき資源数が非常に多かったり, ローカルアカウントがない場合も
  - 情報サービスシステムによるサポート
    - Globus Toolkit 4では, WSRFに基づく汎用情報サービスMDS4を提供
    - Gangliaは管理下の計算ノード群の負荷やメモリ使用量等の資源情報をWebベースまたはMDSを介して提供
- 全てのユーザに対して全ての情報を公開

# グリッド情報サービスの技術的課題

- 個々のユーザやその仮想組織等により、開示する情報を細粒度で制御することが重要
    - 複数仮想組織のユーザが資源を共有する場合、全情報を全ユーザに開示することは好ましくない
    - 商用サービスとして多様なユーザに資源を共有させている場合はなおさら
    - 情報の公開ポリシーはサイトごとに決定
- サイトごとに細粒度のアクセス制御が可能な情報サービスシステムを提案

# 本研究の概要

- 認可に基づく情報サービスシステムの提案
  - 認可モデルとポリシー記述言語の標準であるXACML (eXtensible Access Control Markup Language)を用いる
  - サイトごとに情報開示ポリシーを定義
  - 細粒度の情報アクセス制御が可能
  - WSRF (Web Services Resource Framework)に基づくインタフェースを提供
- Globus Toolkit 4とサンマイクロシステムズのXACML参照実装でプロトタイプを開発・評価
  - XACMLのオーバーヘッドはポリシー数が多い場合も十分小さい
  - 複数サイトから情報収集する場合も、その所要時間は許容できる

# 発表内容

- XACMLの認可モデルとコンテキスト
- WSRFに基づく情報サービスシステム
  - システムモデル
  - 情報取得プロセス
  - 情報サービスシステムの応用と実装
- 予備実験
  - 情報収集・取得の所要時間
  - XACMLの認可判定オーバーヘッド
- 関連研究
- まとめと今後の課題

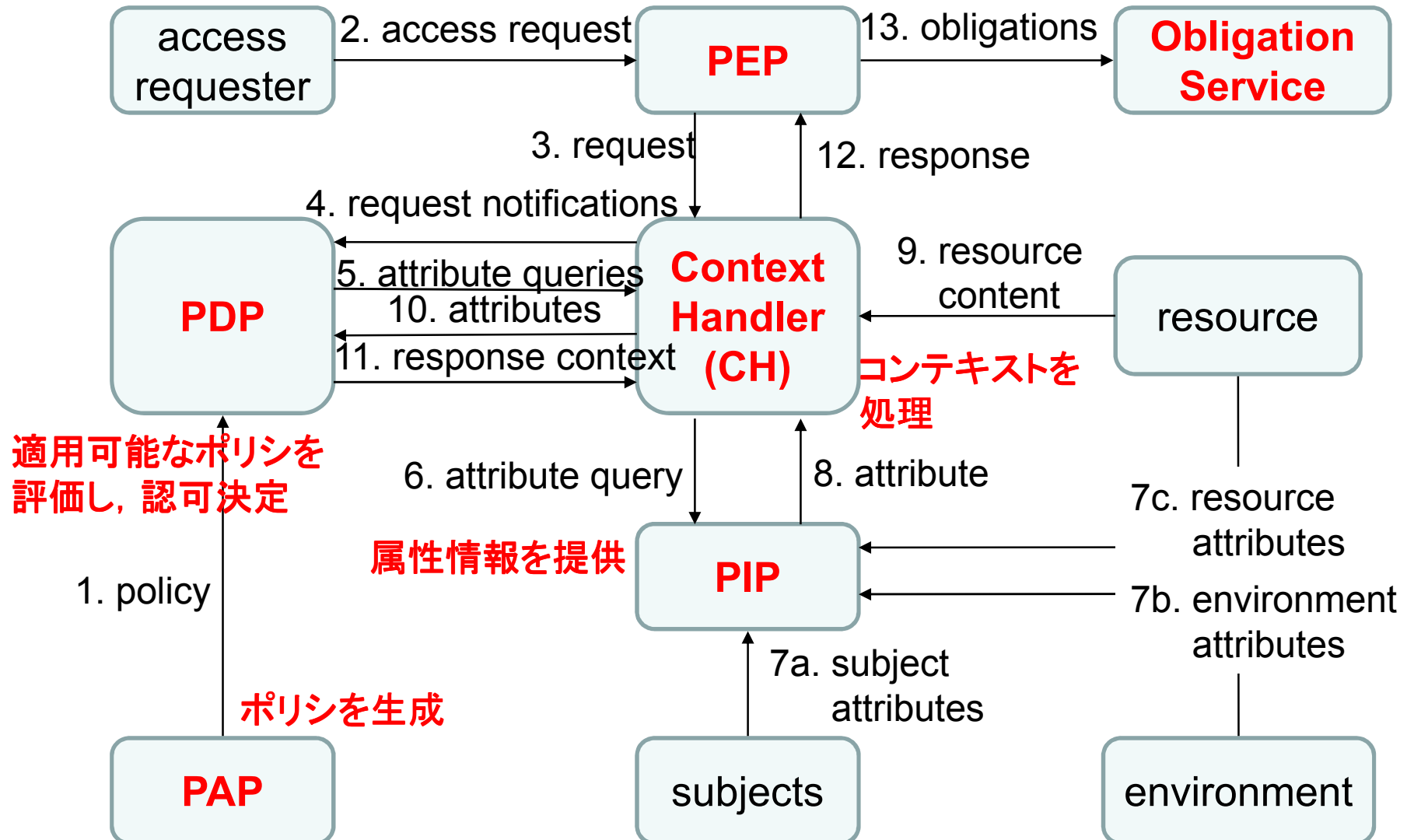
# ウェブサービスのセキュリティ (認証・認可)に関する標準

- SAML (Security Assertion Markup Language)
  - 異なるセキュリティドメイン間でのシングルサインオン
  - 認証・ユーザ属性・認可決定を記述するためのXML
  - リクエスト/レスポンスプロトコルとSOAPバインディング
- XACML (eXtensible Access Control Markup Language)
  - 認可モデル
  - 認可決定を下すのに用いるルールを表現するXML

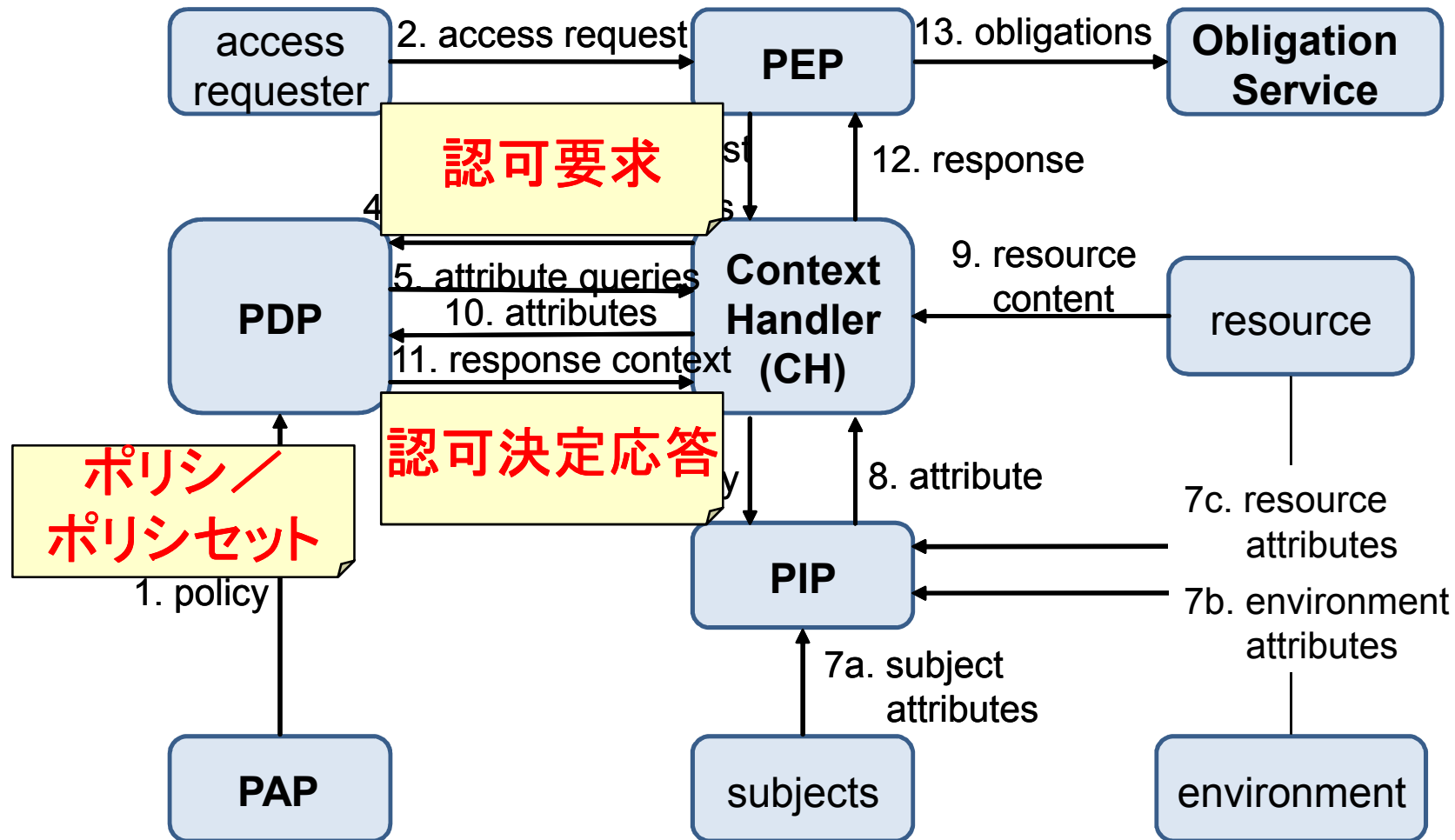
# XACMLの認可モデル

認可決定に基づき  
アクセス制御

指定された  
仕事を行う



# XACMLのコンテキスト



# 認可要求

```
<?xml version="1.0" encoding="UTF-8"?>
<Request>
  <Subject>
    <Attribute AttributeId="属性識別子"
      DataType="属性の型">
      <AttributeValue>属性値</AttributeValue>
    </Subject>
    <Resource>
      <Attribute AttributeId="属性識別子"
        DataType="属性の型">
        <AttributeValue>属性値</AttributeValue>
      </Resource>
      <Action>
        <Attribute AttributeId="属性識別子"
          DataType="属性の型">
          <AttributeValue>属性値</AttributeValue>
        </Action>
      </Request>
```

<Subject> : 誰が  
<Resource> : 何に対して  
<Action> : 何を行いたいのか

# ポリシー/ポリシーセット

```
<Policy PolicyId="ポリシー識別子"
  RuleCombiningAlgID="アクセス可否の判定方法">
  <Description>ポリシーの説明</Description>
  <Target>ポリシーを適用する要求</Target>
  <Rule>判定規則</Rule>
</Policy>
```

```
<PolicySet PolicySetId="ポリシーセット識別子"
  PolicyCombiningAlgID="アクセス可否の判定方法">
  <Description>ポリシーセットの説明</Description>
  <Target>ポリシーセットを適用する要求</Target>
  <Policy>ポリシー(直接記述)</Policy>
  <PolicyIdReference>既存ポリシーのID (参照)
  </PolicyIdReference>
</PolicySet>
```

## Policy

<Target>でポリシーを適用する要求を指定

- <Subject>, <Resource>, <Action>が記述可能

<Rule>で判定規則を記述

- 複数記述可能
- RuleCombiningAlgIDで判定方法を指定

PolicySet : 複数ポリシーを同時に適用する場合に利用

- PolicyCombiningAlgIDで判定方法を指定
- 複数ポリシーの指定方法
  - Policy, PolicySetを直接記述
  - <Policy/SetIdReference>でIDを指定

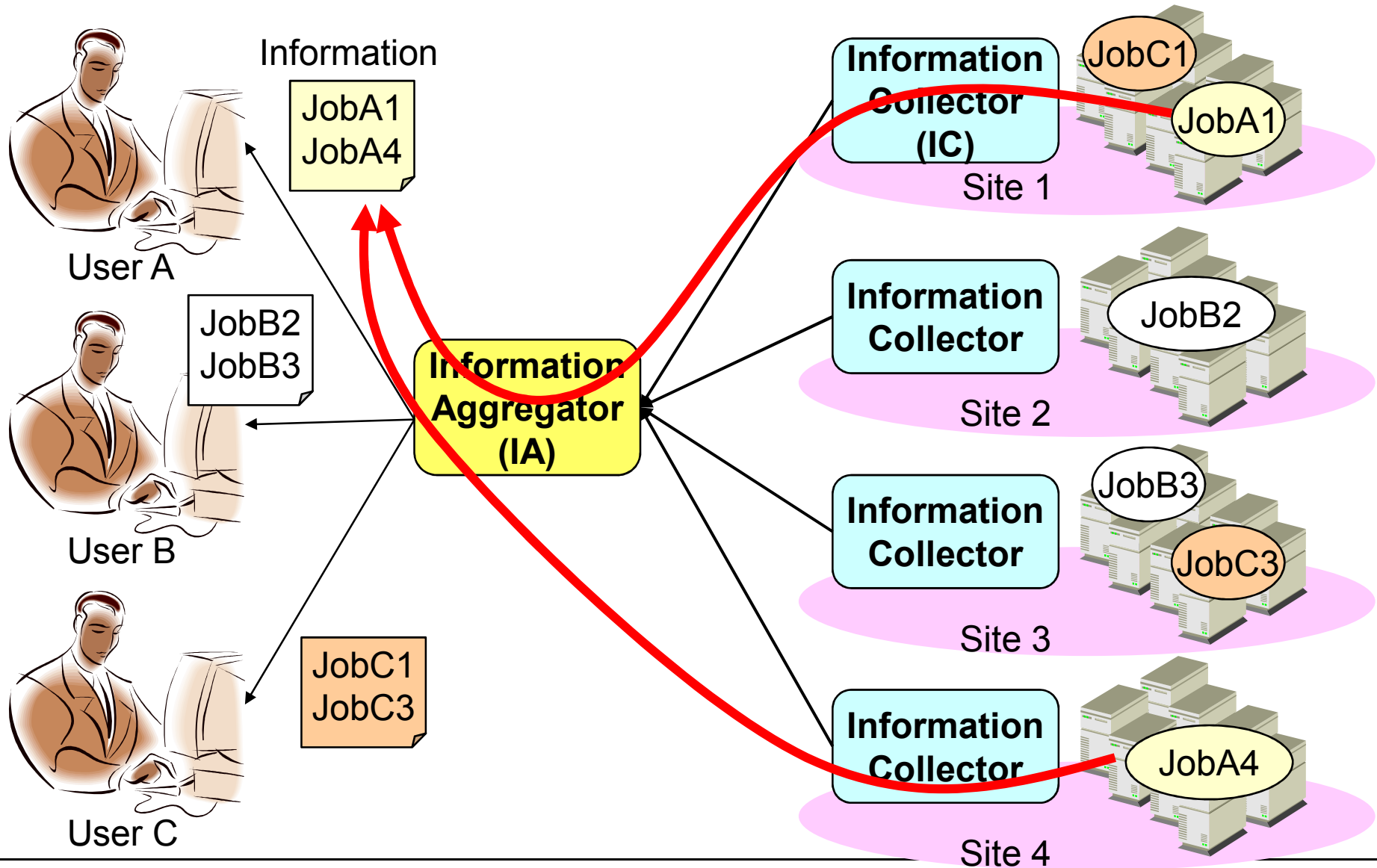
# 認可決定応答

```
<Response>  
  <Result>  
    <Decision>認可決定結果  
  </Decision>  
  </Result>  
</Response>
```

<Result>タグ下の  
<Decision>で結果を記述  
以下のいずれかを返す

- Permit (認可)
- Deny (否認)
- Indeterminate (評価過程で構文エラー発生)
- NotApplicable (適用するルールなし)

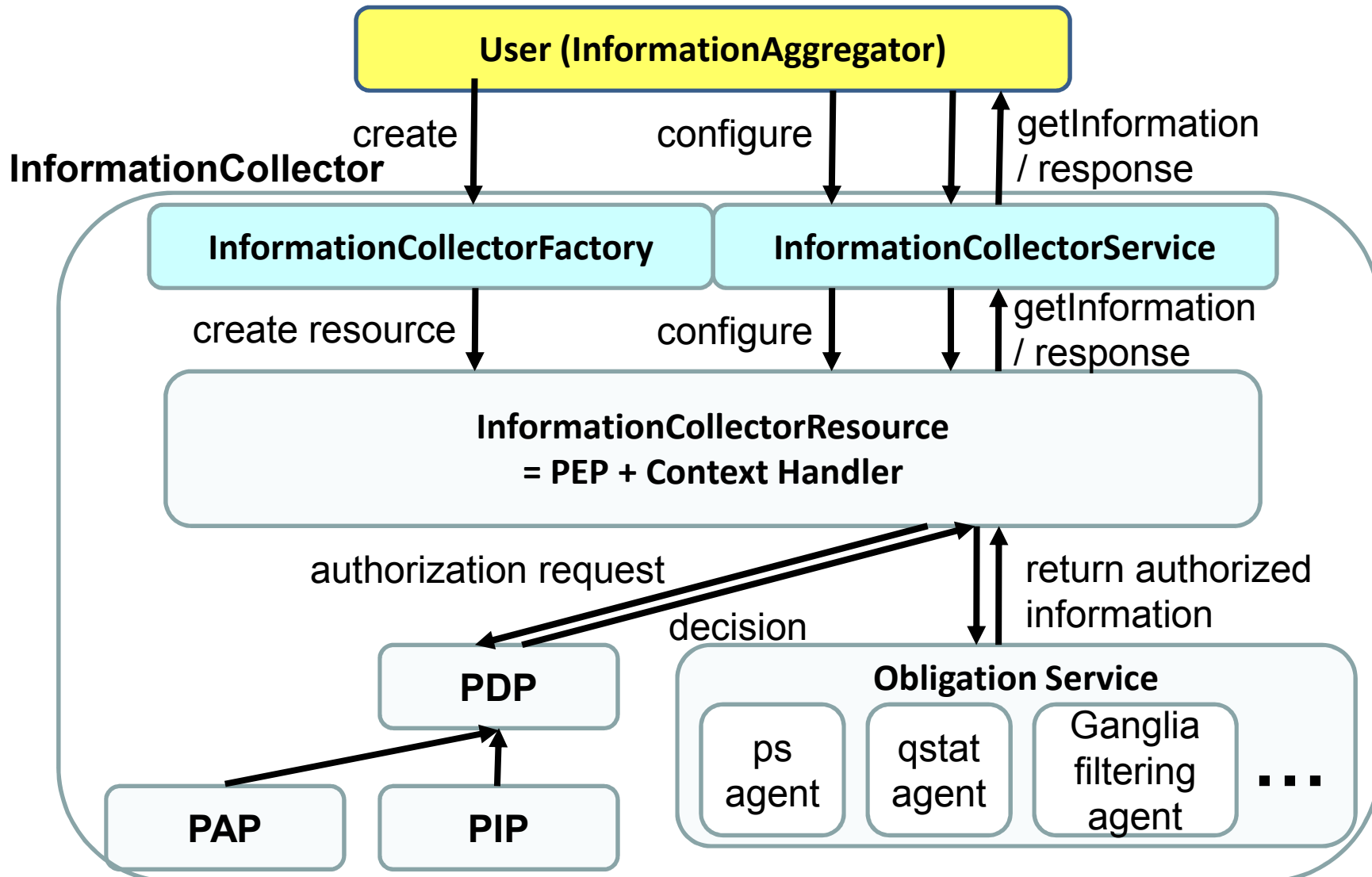
# 情報サービスシステムモデル



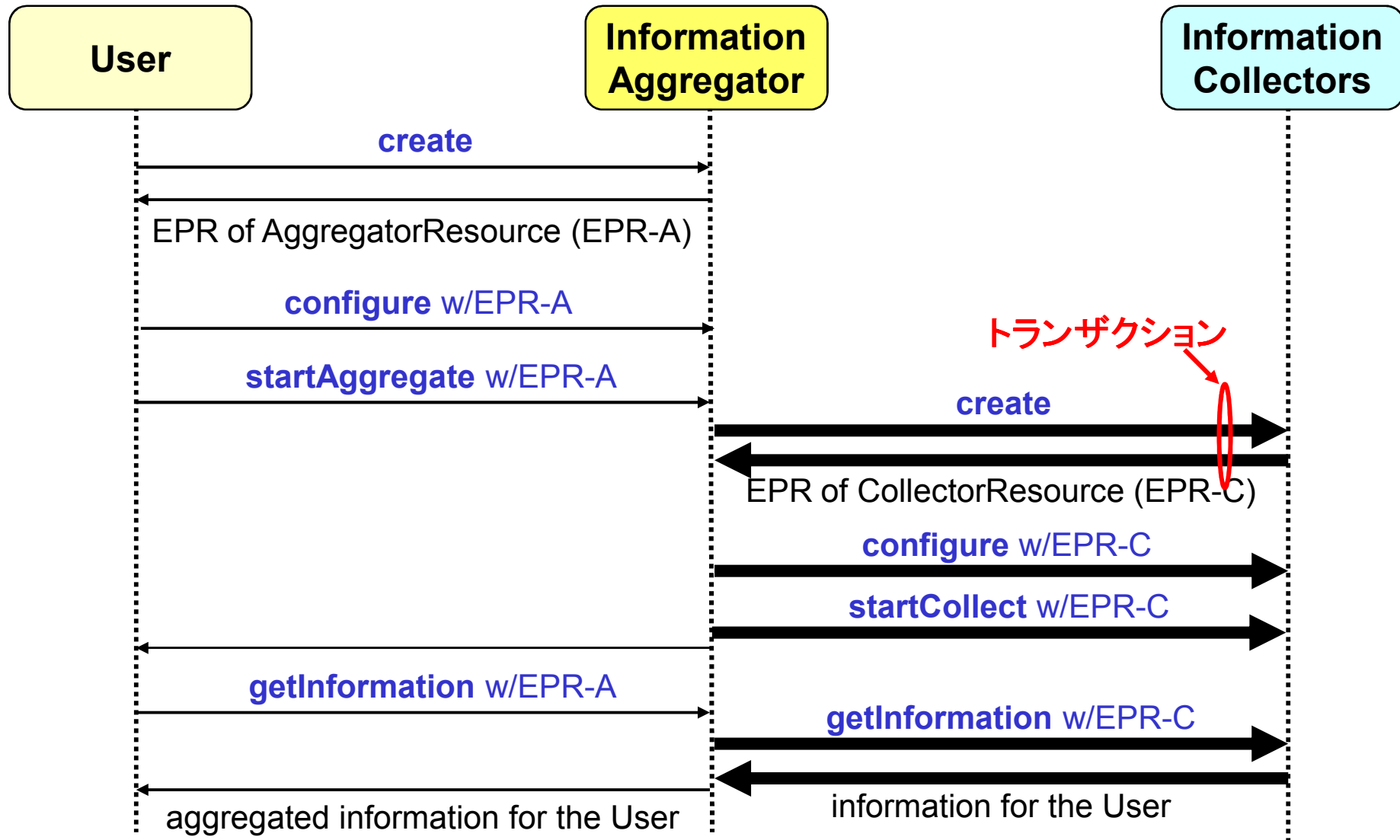
# InformationCollector (IC)

- ICでのみ認可決定手続きを行う
  - 認可されていない情報をサイト外に流出させない
  - XACMLの認可モデルに基づき設計
- ICの構成
  - WSRFインタフェースモジュール  
(InformationCollectorFactory/Service)
  - ステートフルサービスインスタンスモジュール  
(InformationCollectorResource (ICR))=PEP + CH
  - 認可決定関連モジュール(PDP, PAP, PIP)
  - Obligation Serviceモジュール
    - 各情報に対応したエージェントを用意し、動的／静的な情報を提供
    - サイト管理者が開示したい情報を予め登録

# InformationCollectorアーキテクチャ



# WSRFに基づく情報取得プロセス



# 情報サービスシステムの応用

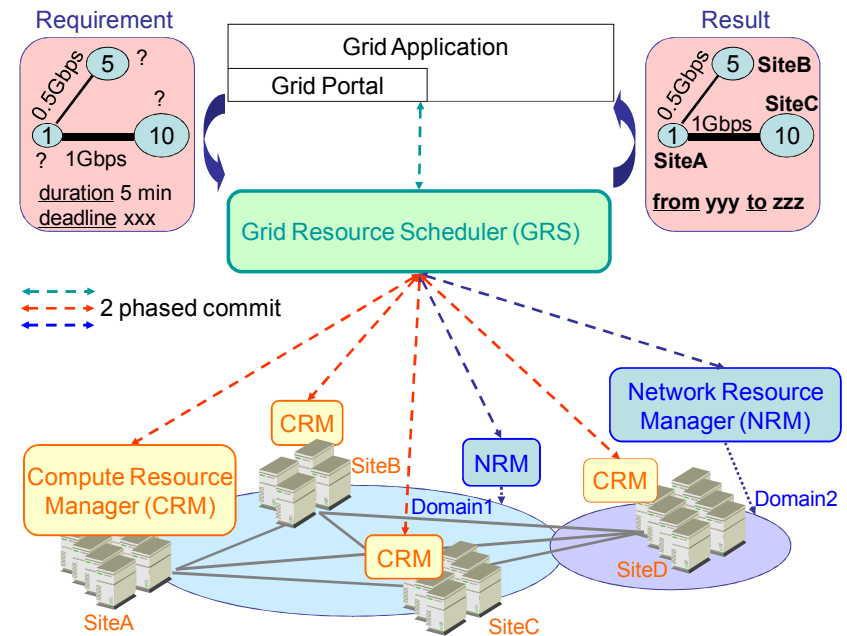
- 事前予約に基づくグリッドコアロケーションシステムとの連携

- GridARS (Grid Advance Reservation-based System framework)

- WSRF I/F
    - GRSと事前予約機能付き資源マネージャ(RM)で構成
    - GRSが複数RMと連携し、ユーザの要求した資源を事前予約で確保
    - 予約時刻に確保した資源を自動的に利用可能に

- GRSの管理する予約情報を取得し、予約時刻に予約資源情報を提供することが可能

- GRSの予約サービスインスタンスへのポインタ(EPR)を利用



# 情報サービスシステムの実装

- WSRFモジュール - [Globus Toolkit 4 \(GT4\)](#)
  - GSI (Grid Security Infrastructure)を利用
    - ユーザ認証
    - grid-mapfileによるグローバル/ローカルユーザ名のマッピング情報取得
    - SSLでのセキュア通信
    - 権限委譲(ユーザはIAとのやり取りのみでよい)
- XACMLモジュール - [XACML Java参照実装 \[サンマイクロシステムズ\]](#)
  - XACML ver 1.xに対応
  - ポリシ検索モジュールを別途実装し, PDPを適宜構築  
→適宜ポリシを追加・修正することが可能

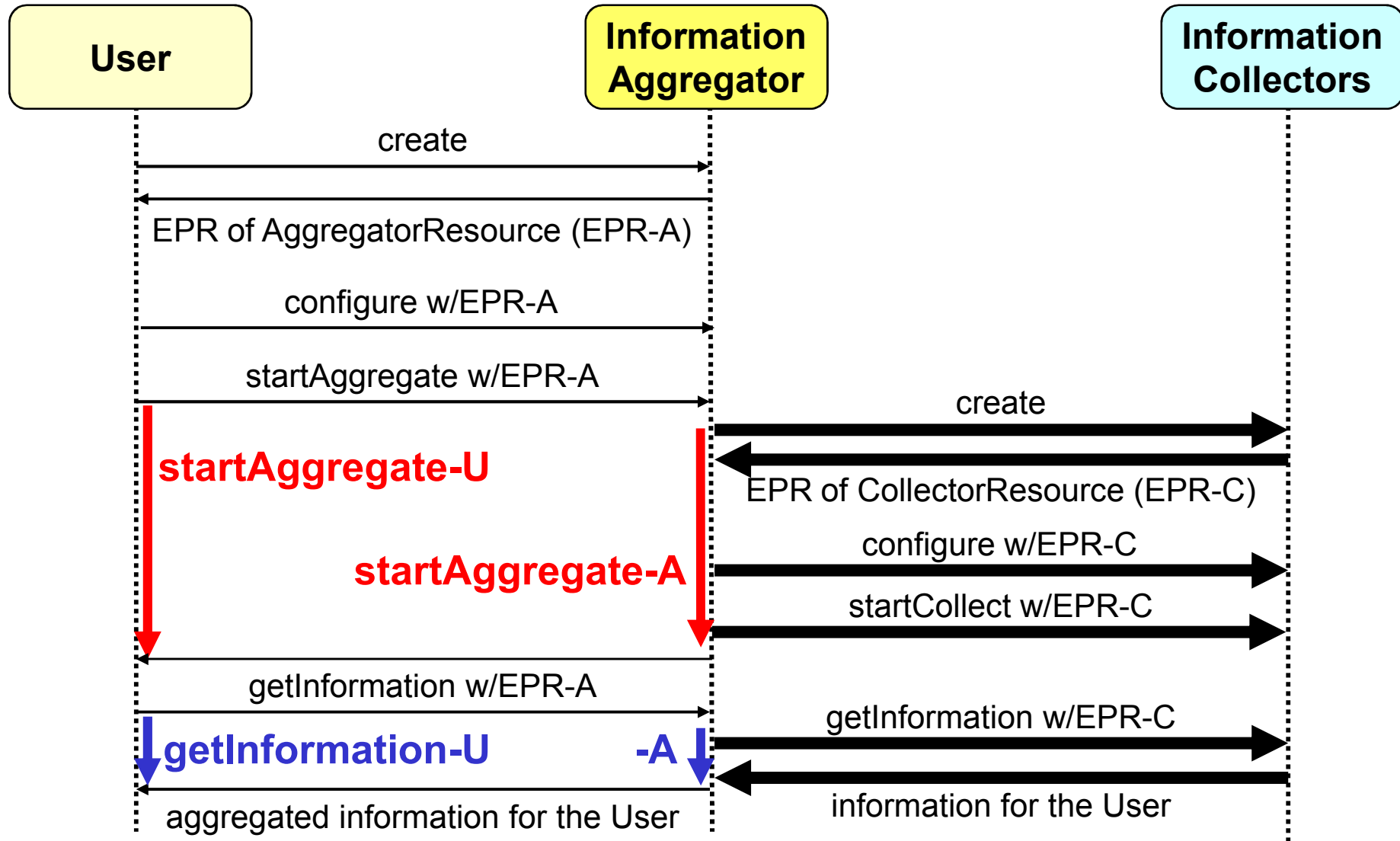
# 予備実験

- 情報サービスシステムプロトタイプを用いた評価
- 実験1: 情報収集・取得の所要時間
  - WSRF/GSIでの情報収集・取得時間を調査
  - IAとICが1対1と1対7の場合の比較
- 実験2: XACMLの認可判定オーバヘッドの測定
  - ポリシ数に対する所要時間の調査

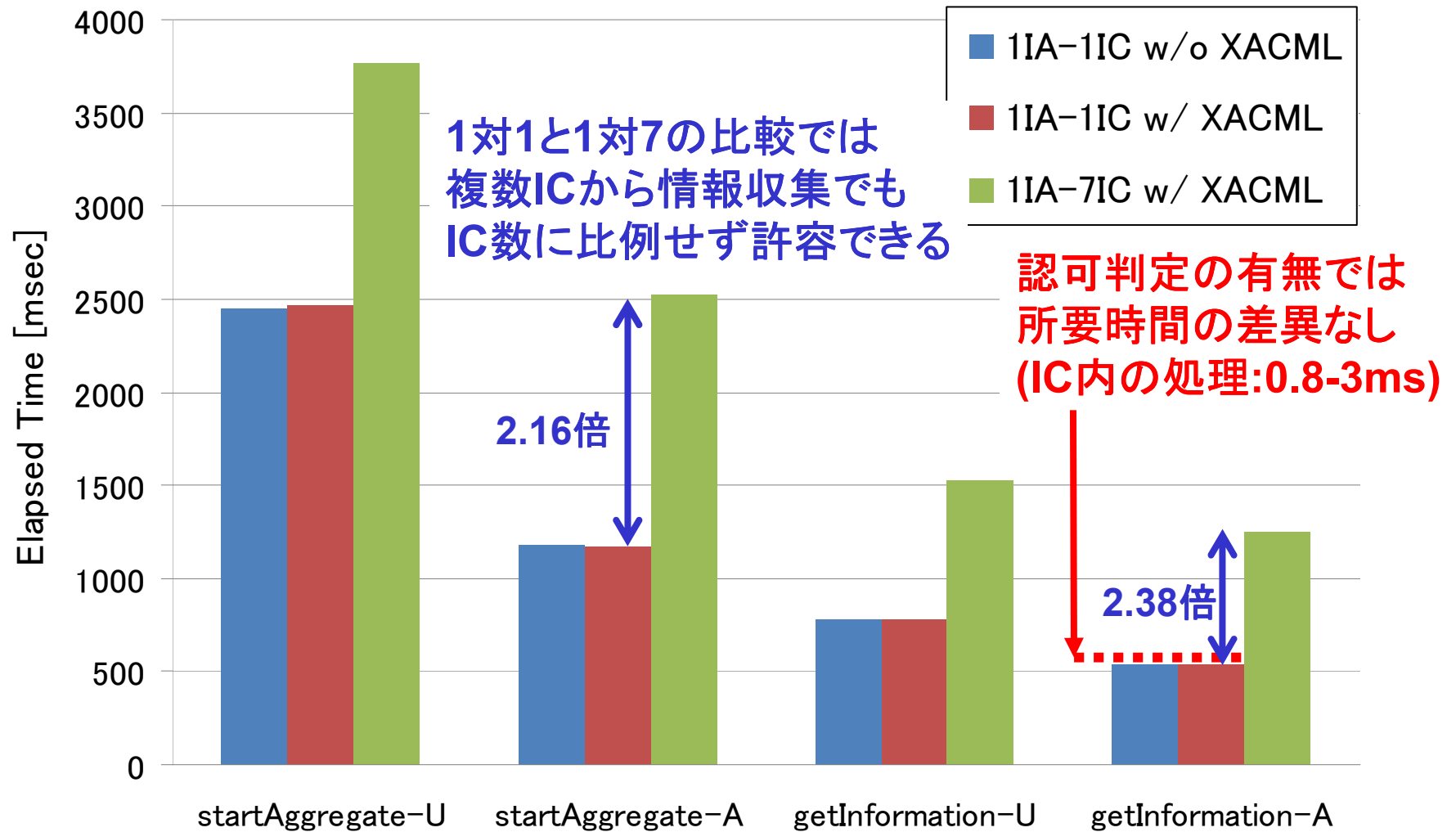
# 実験環境

- 実験環境
  - ユーザとIAは同一ホスト, ICはそれぞれ別ホスト
  - IA, ICは同じクラスタ内に設置
  - 全ホストは1つの1Gbpsスイッチに接続
  - 各ホスト間の遅延は40us
  - 全ホストの構成 : Pentium 4 2.8GHz, 1GBメモリ, CentOS4.3
- 利用したポリシーセット
  - ユーザ証明書のDNがgrid-mapfile内にあるか
  - 予め指定した時刻内の問い合わせか

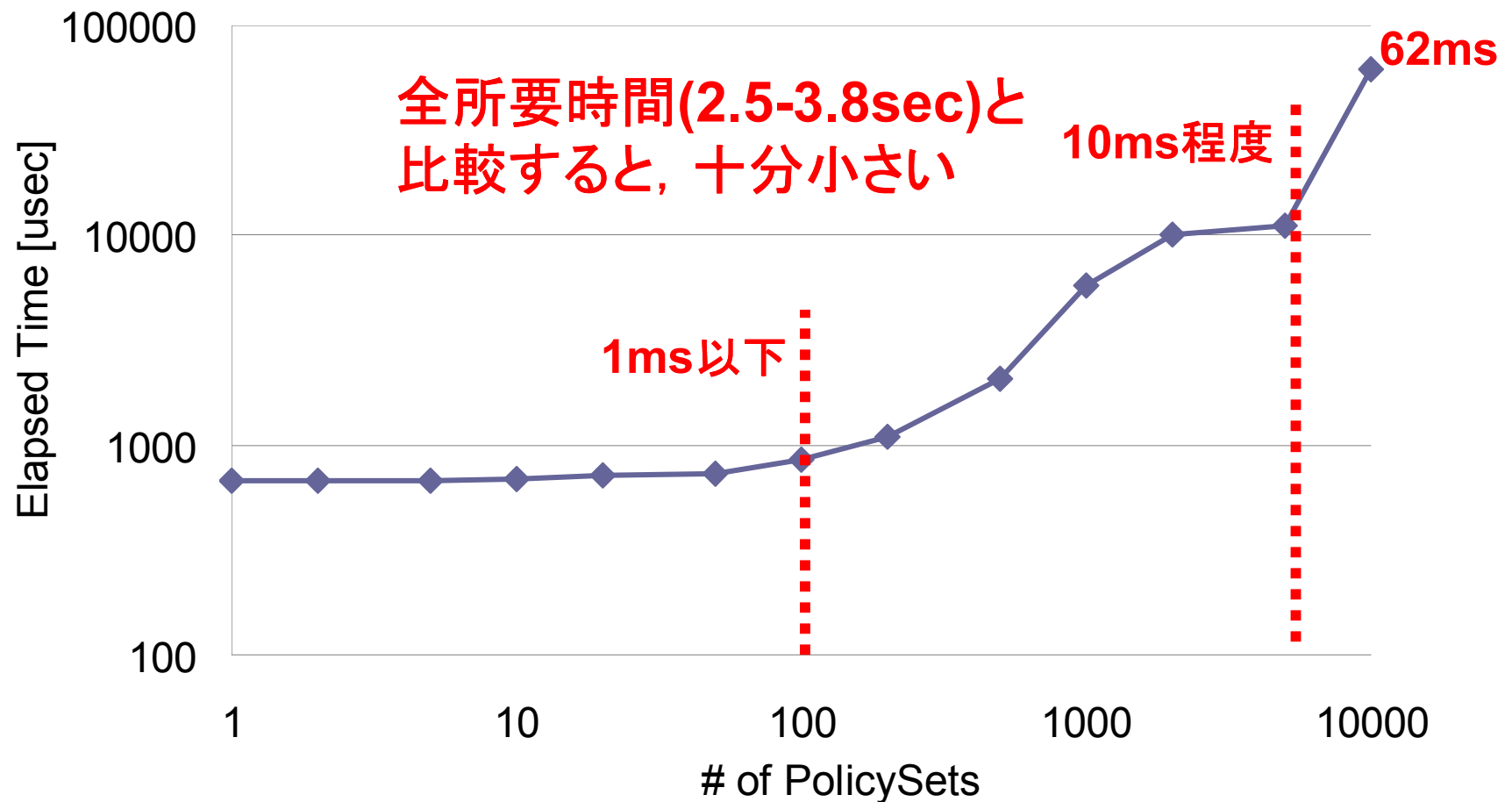
# 実験1: 情報収集・取得の所要時間の比較



# 実験1: 情報収集・取得の所要時間



# 実験2: XACMLの認可判定オーバーヘッドの測定



# 関連研究

- **Globus Toolkit 4 [Lang, NCA06]**
  - WSRFに基づくサービスのリソースへのアクセス認可をXACMLに基づいて行う
  - 認可の粒度がリソース単位で粒度が大きい
  - GT4.2以降で公開予定
- **MonALISA [Harvey, CHEP2001]**
  - GangliaやMRTG等で収集された情報をレポジトリに格納し, GUIで提供
  - 認証のみで, レポジトリ内のデータは全ユーザがアクセス可能
  - ウェブサービスI/F
- **Inca [Smallen, SC2004]**
  - TeraGridで使われているユーザレベルグリッドモニタリングシステム
  - 複数サイトの情報を集中管理するため, サイト外に収集情報が流出
  - サイトごとのアクセス制御なし

# まとめ

- 認可に基づく情報サービスシステムの提案
  - 認可モデルとポリシー記述言語の標準XACMLを用いる
  - サイトごとに情報開示ポリシーを定義
  - 細粒度の情報アクセス制御が可能
  - WSRFに基づくインタフェースを提供
  - InformationAggregatorと認可に基づく情報提供を行うInformationCollectorで構成
  - GT4とサンマイクロシステムズのXACML参照実装を用いてプロトタイプを開発
- 評価実験
  - XACMLのオーバーヘッドはポリシー数が多い場合も十分小さい
  - 複数ICから情報収集する場合も、その所要時間は許容できる

# 今後の課題

- 多様なアクセス制御ポリシーの適用
- 情報サービスシステムとGridARSコアロケーションフレームワークとの連携
- ユーザインタフェースの構築

# 謝辞

- 本研究の一部は，文部科学省科学技術振興調整費「グリッド技術による光パス網提供方式の開発」による。