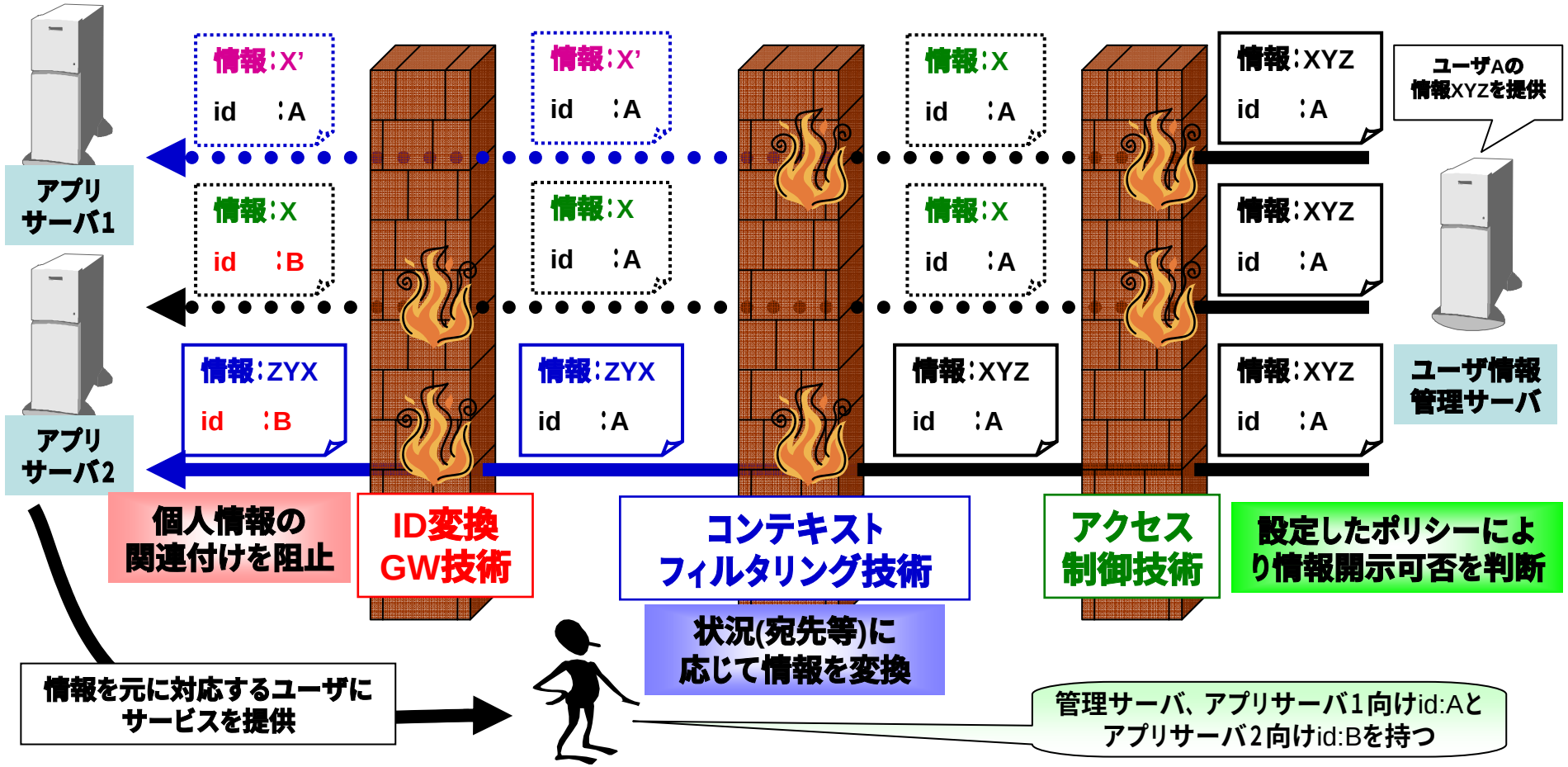
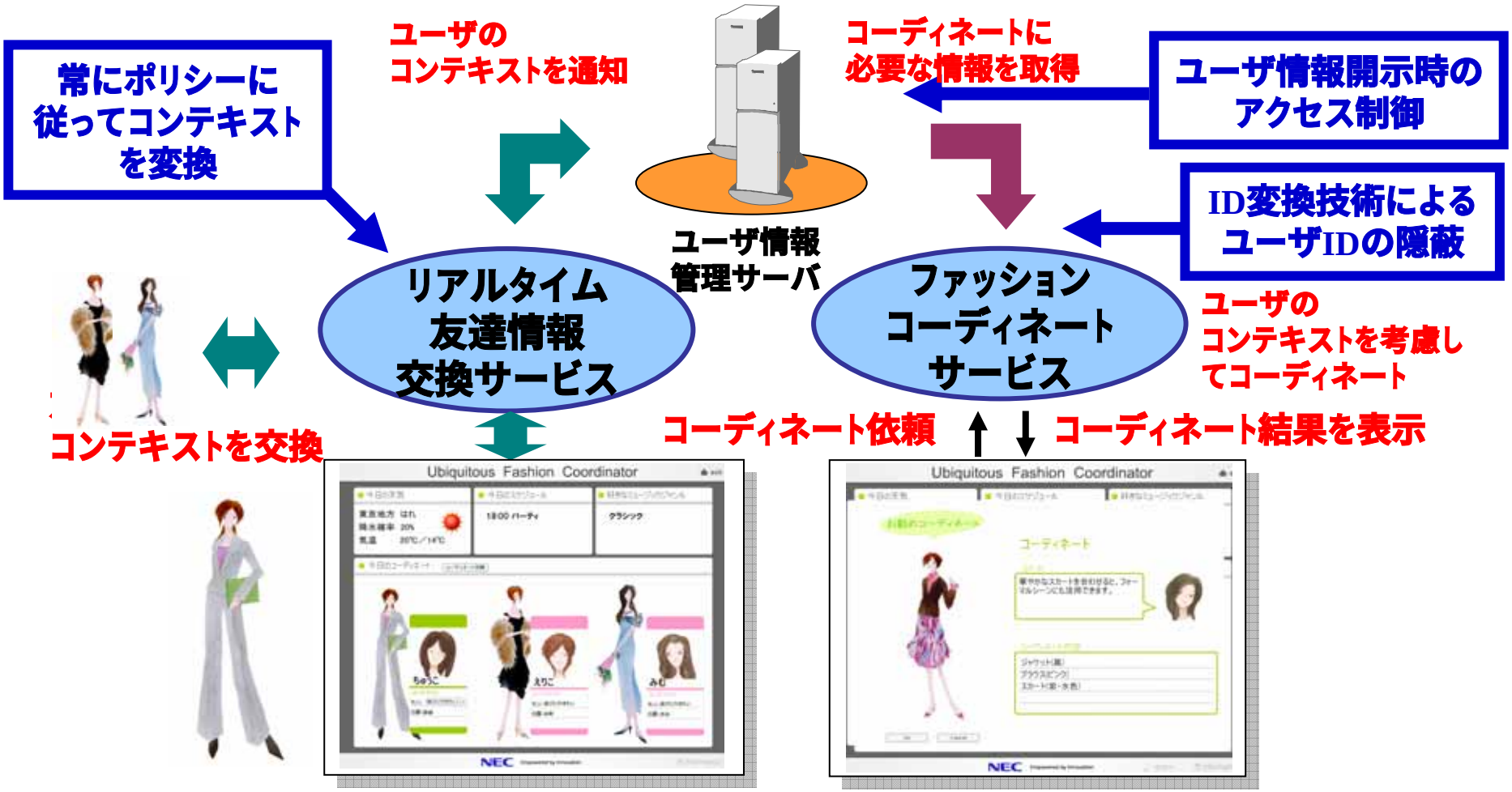
（T3）プライバシを考慮した情報流通

ユビキタスサービスの展開では、ユーザがいつでも便利なサービスを安心して受けられるようにしなければなりません。このため、サービスを受けるために必要なプライバシを含むユーザ情報を保護する技術を開発・検証しました。

【技術概要】



【実現例】
リアルタイムに友人間で情報を交換するサービスから獲られた情報（友達の服装）とユーザ情報管理サーバのユーザ情報（ワードローブ、スケジュール、友達の服装、お気に入りの音楽ジャンル）から、必要な情報だけを提示し、お勧めのファッションを受けるファッションコーディネートサービスを受けるシステムを、それぞれの技術を利用して実現しました。



★ 友達と気分･位置･服装などの情報を交換
★ 友達によって異なる気分を見せられる

★必要な情報だけを提供してファッションコーディネートサービスを受ける

【技術説明】

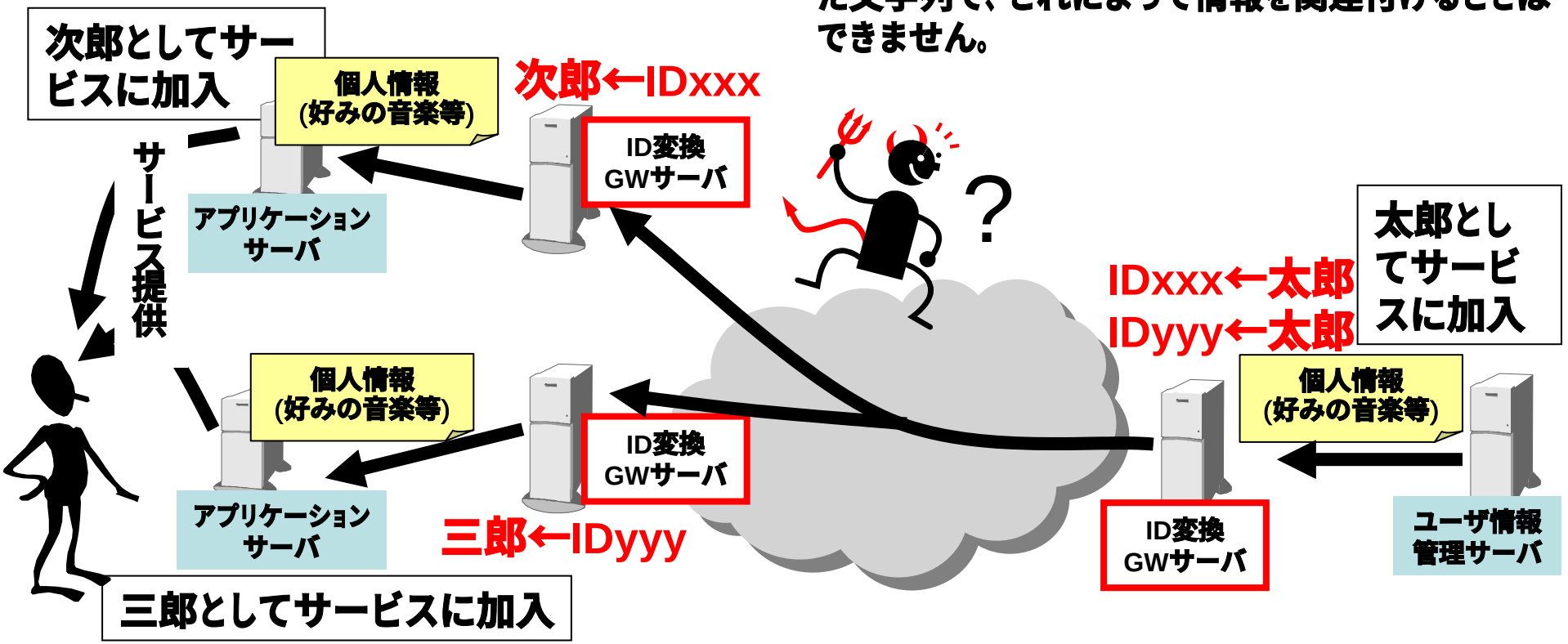
トラッキング防止技術（ID変換GW技術）

概要

- ユーザは複数のサービスに個人情報を提供
- ユーザの意図しない複数の情報の関連付けを防止するため情報取得の際にGWでユーザIDを変換

特徴

- あるサービスが持つあるユーザの情報を、個人を特定することなく他のサービスが取得することができます。
- 取得の際に用いるユーザIDは一時的に生成された文字列で、これによって情報を関連付けることはできません。



【技術説明】

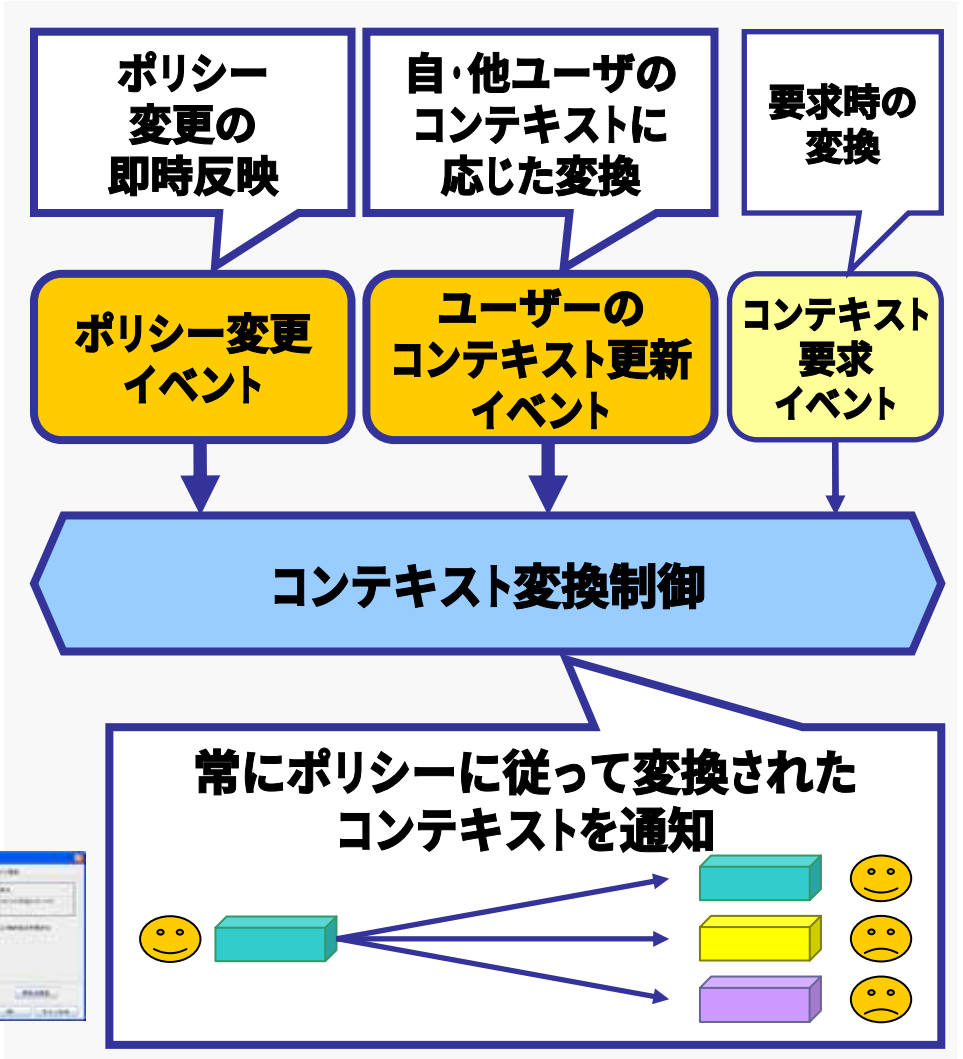
コンテキストフィルタリング技術

概要

- 継続的にコンテキストを交換する環境において、常にポリシーに従ったコンテキスト変換、通知をすることで、ユーザのプライバシを保護

特徴

- コンテキストを監視中の相手に対して即時にポリシーの変更を反映
- 自・他ユーザのコンテキスト変化に応じて自動的にコンテキスト変換動作を変更
  - 動的な変更によるプライバシ情報の漏洩を回避
- GUIによる簡単ポリシー設定

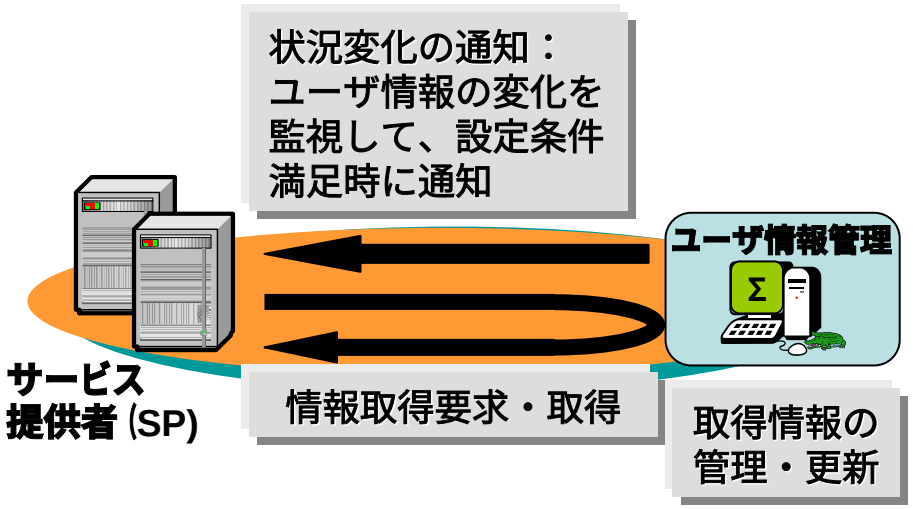


【技術説明】

情報アクセス（開示情報）制御

概要

- ユーザは複数サービスに個人情報を提供
- ユーザ情報管理サーバへ外部からアクセスした際に、アクセス元や提供サービスに応じて、開示可否を判断



(*)eXtensible Access Control Markup Language

特徴

- XACML(*)をもとにしたポリシ設定
  - 個々の要素毎にPermit/Denyを判断
  - 各SPに対し初期ポリシを選択。その後の利用履歴によりポリシを修正。
  - 粒度を有するデータの取り扱いも可能。

◆ ユーザ初期設定

SP-A：5
SP-B:4
SP-C：3

※SP=Service Provider

◆ デフォルトのポリシ

	日本語名	Permit	Deny
フィールド1	氏名	5，4	3，2，1
フィールド2	姓	5，4	3，2，1
フィールド3	名	5，4，3	2，1
フィールド4	性別	5，4	3，2，1
フィールド5	携帯電話番号	5，4，3	2，1

利用履歴を考慮
SP-Aのポリシを変更

◆ ユーザ毎のポリシ

許可項目	対象	不許可項目	対象
フィールド1 Permit	SP-A, SP-B	フィールド1 Deny	SP-C
フィールド2 Permit	SP-A, SP-B	フィールド2 Deny	SP-C
フィールド3 Permit	SP-A, SP-B, SP-C	フィールド3 Deny	
フィールド4 Permit	SP-A, SP-B	フィールド4 Deny	SP-C
フィールド5 Permit	SP-A, SP-B, SP-C	フィールド5 Deny	