

ユビキタスネットワーク認証・ アクセス制御技術の研究開発

Dec. 2005

(株)日立製作所

ユビキタスネットワーク認証・エージェント技術



膨大な要素数の動的なネットワーク環境に適用できる高性能認証プラットフォーム, サブネットワークやノードの移動をユーザに隠蔽する高速認証, 状況の変化に対して回路レベルで自律適応する機器構成技術, その場その時そのユーザに適したサービスを合成する超分散サービス合成エージェント, 過去/現在/未来のプロフィールに応じたコンテンツ推薦や低機能端末の適応的ルーチングなどの新規技術を研究開発

代表研究責任者 (NTT 須田宏一 NS研所長)

ア) 大量モビリティ対応認証技術
イ) 分散型認証制御技術



ウ) 自律分散ノード認証技術



エ) 自律適応型ネットワークシステム構成エージェント技術



オ) コンテンツ流通エージェント技術



ア) 大量モビリティ対応認証技術

■ コンテキスト・アウェア利用者認証

- 従来の集中型サーバによる画一的な認証ではなく、利用場所の状況やセキュリティレベルの変化に対応して利用者の認証・認可処理を複数のエージェントに分散して代行することが可能な、柔軟かつスケーラブルな認証技術の開発

■ 異種レイヤ/ドメイン間認証連携

- セキュリティポリシーの異なるレイヤ間／ドメイン間で認証関連情報を安全に交換してシングルサインオンを行い、移動時にもアプリケーションやサービスをシームレスに利用可能とするネットワーク認証連携技術の開発

イ) 分散型認証制御技術

■ アクセス制御ポリシー自動構成

- 利用者や利用場所の状況によって変化する、情報機器・サービスへのアクセス、データの暗号化・消去などのセキュリティ確保、ユーザへのリソース割り当て等を行う制御ルールを自動生成し、リアルタイムに設定可能なアクセス制御技術の開発

■ 仮想アクセス空間・構成

- 認証制御エージェントからの要求に応じて動的な通信経路を確立し、大量の認証情報・コンテキスト情報を高速に伝達可能なネットワーク制御技術の開発

今年度の取り組み



■ 認証・アクセス制御プラットフォームの確立

- ① 16年度に開発した機能コンポーネントであるマルチモーダルな認証クライアント、状況依存型ポリシーエンジン、エージェント間認証連携、アクセス制御ポリシー生成・配布を統合したプラットフォームを構築し、実験評価・改良を実施。
- ② 実用化の観点から、数十～百エージェントが相互に連携動作しても性能劣化をおさえるために連携プロトコルを改良し、100万ユーザ規模のスケーラビリティを達成。エージェントによる信頼NWを動的に確立する機能を新たに開発。
- ③ コンテキストエージェントによるポリシー高度化や設定を容易化するインターフェース機能を開発。制御可能な機器・サービスの数を増やせるよう設定プロトコルを改良。
- ④ 共通的な認証・アクセス制御API及び実行基盤を提供することにより、グループ内連携を進め、1000ユーザ規模でのフィールド実験を通して成果の公開を図る。

■ 仮想アクセス空間・構成技術の開発

- 16年度に開発したリンク管理プロトコルの性能評価、改良を進める。端末数が100万台に増加した場合でもスケーラビリティを確保するため、認証トラフィック負荷分散方式、エージェント間のコンテキストDB同期化方式を開発する。

ネットワーク環境のパラダイムシフト



	従来のネットワーク環境	ユビキタスネットワーク環境
ユーザ、デバイス	事前登録されている、 管理主体はひとつ	必ずしも事前登録されていない(自動認識や自動発見が必要)、複数の 管理主体が混在
ネットワーク接続	場所に固定的な接続、同一の ネットワークやセキュリティドメイン 内でのアクセス(ファイヤー ウォールによる防御)	場所を移動しながら接続、ネットワー ク境界やセキュリティ境界をまたがる アクセス(物理的持込みやリモートア クセスを許可)
コンピュータ環境	構成や状態の変化が比較的ゆる やか、ユーザやリソースを一 元管理可能	構成や状態の変化が激しい、ユーザ やリソースの管理が分散
コンテキスト管理	プライバシー情報を含むユーザ コンテキストの自動取得は困難	小型センサーの普及によりユーザコ ンテキストの自動取得が容易 → プ ライバシー問題
セキュリティ	ユーザビリティを犠牲にしてもセ キュリティを確保	ユーザビリティやプライバシーとの両 立が必須

研究課題とアプローチ

- ・アクセス集中やNW障害の影響を受けないために認証サーバの分散構成が必要。
- ・ユーザと認証サーバの間のセキュリティ確保を容易にする。



分散エージェント
フレームワーク

- ・常に厳格で画一的な本人確認を行うと利便性が損なわれ、コストがかかる。
- ・安全性を高めるためにセンサ情報を活用し多層的、多角的な防御を行いたい。



状況適応型ポリシー
コントロール

- ・異なるプロバイダが連携して、シングルサインオンやパーソナライズサービスを提供する。
- ・属性認証、匿名アクセスによりプライバシーを強化したい。



ネットワーク認証
連携 (federation)

- ・端末・機器構成がリアルタイムに変わる環境で管理者が事前に設定して管理は困難。
- ・利用環境に応じてユーザ自身がセキュリティをコントロールできるようにしたい。

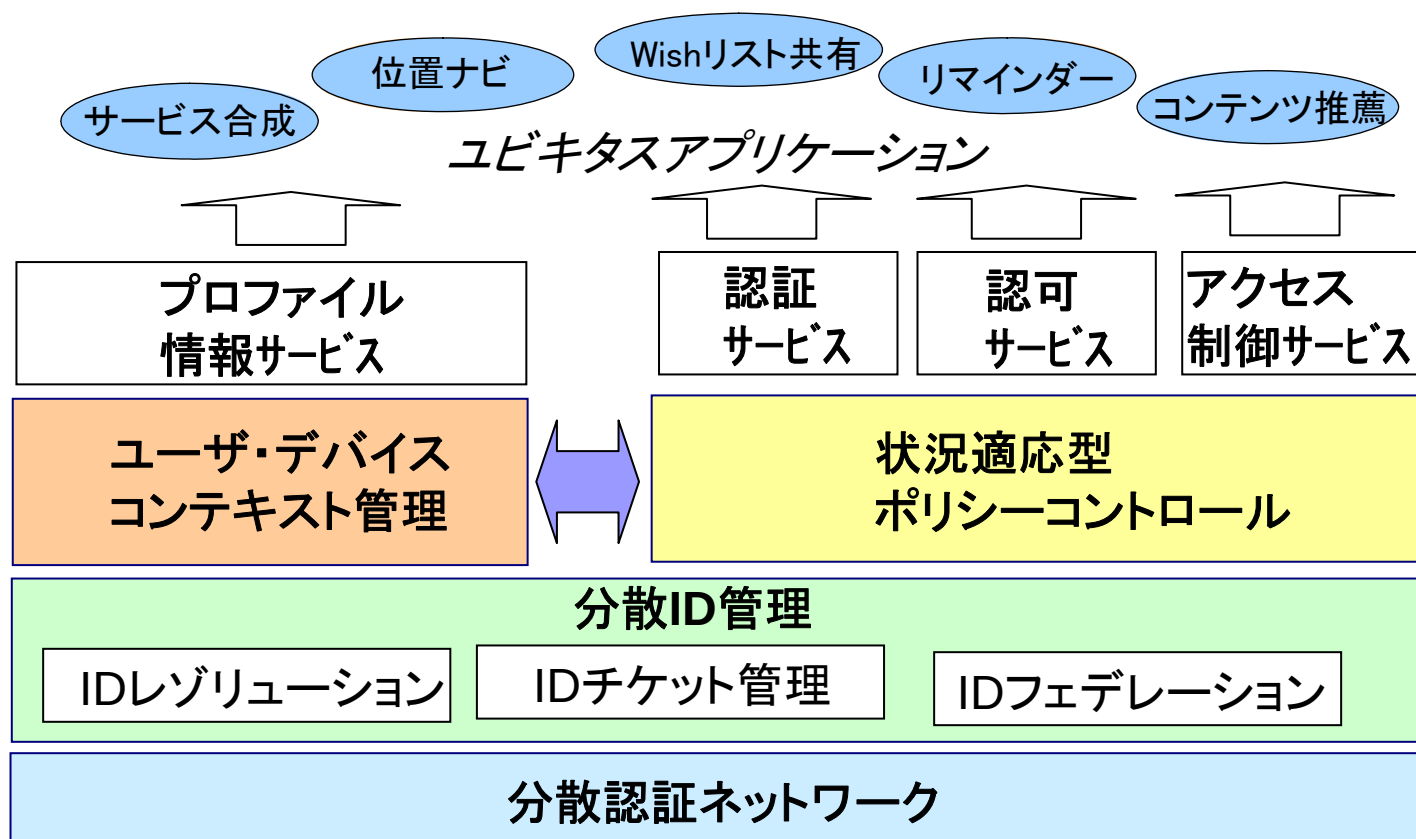


電子チケットによる
サービスアクセス制御

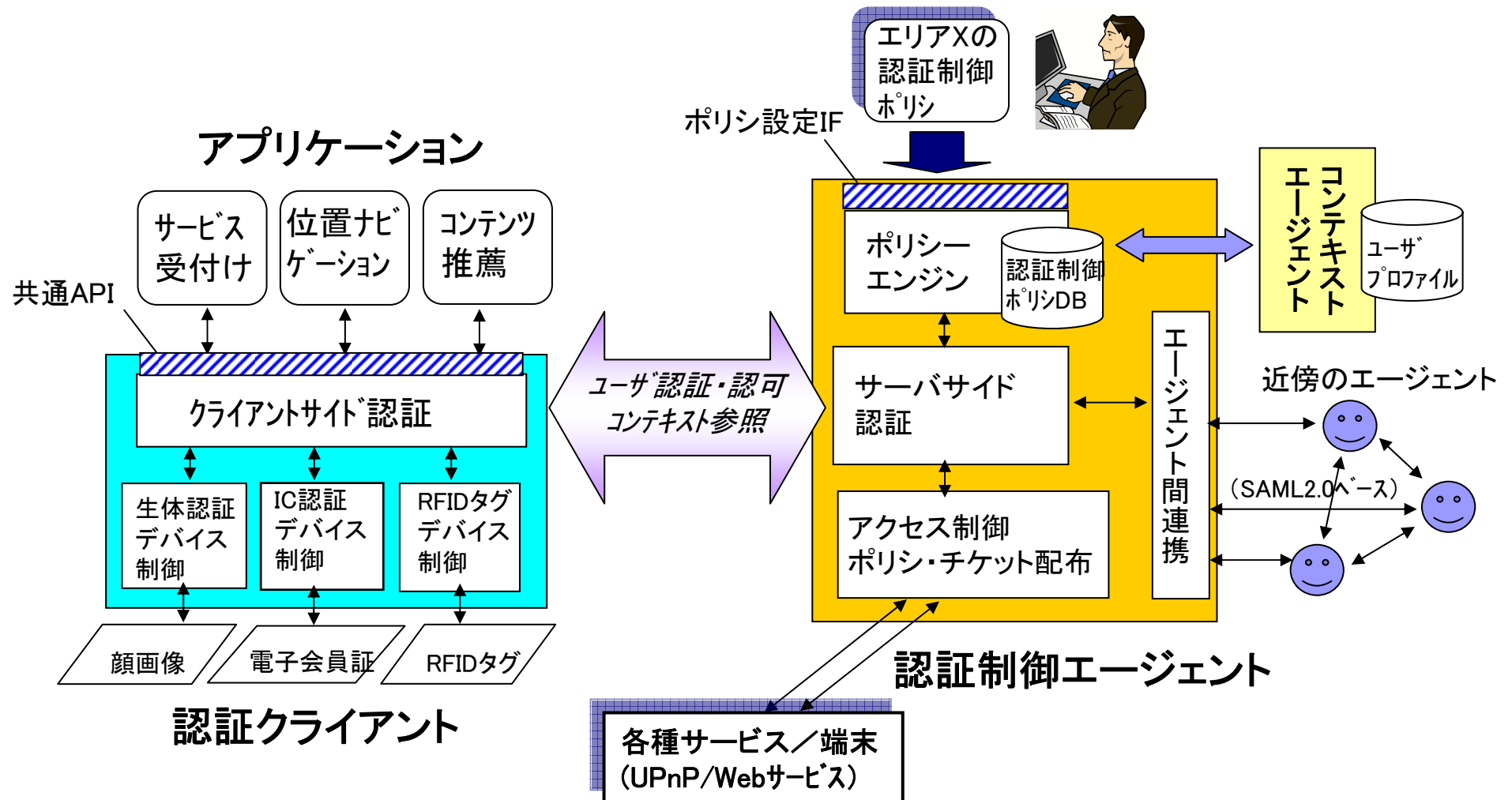
ユビキタス認証制御アーキテクチャ



- サービス連携のためのエンド・ツー・エンドのセキュリティ基盤
- 移動ユーザ・移動端末からの利用を前提とし、セキュアな空間を移動とともに維持
- ID情報・プロフィール情報とコントロールの分離



認証制御エージェントの機能構成



- 状況適応型アクセス制御

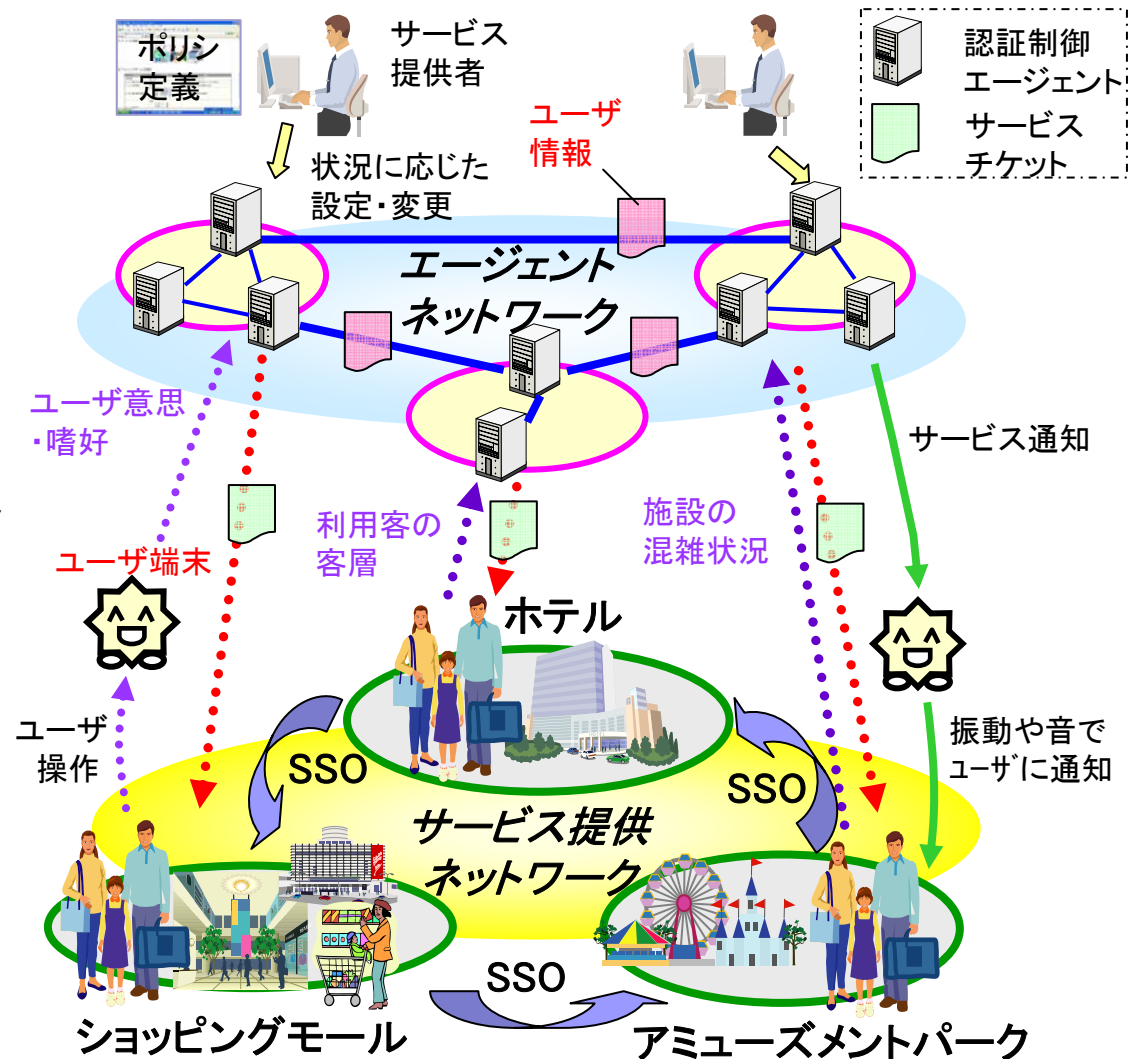
エリアの利用状況をセンシングし、これを反映したサービスチケットを発行することで適切なアクセス制御が可能

- 気付きコミュニケーション

易しい端末操作でユーザの意思（利用したいサービスや信頼するメンバーの登録等）をシステムに反映したり、サービスの存在を近接ユーザに通知

- 分散認証ネットワーク

異なるセキュリティポリシーを持つエージェント間においても、ユーザの情報を共有することにより、シングルサインオンで認証

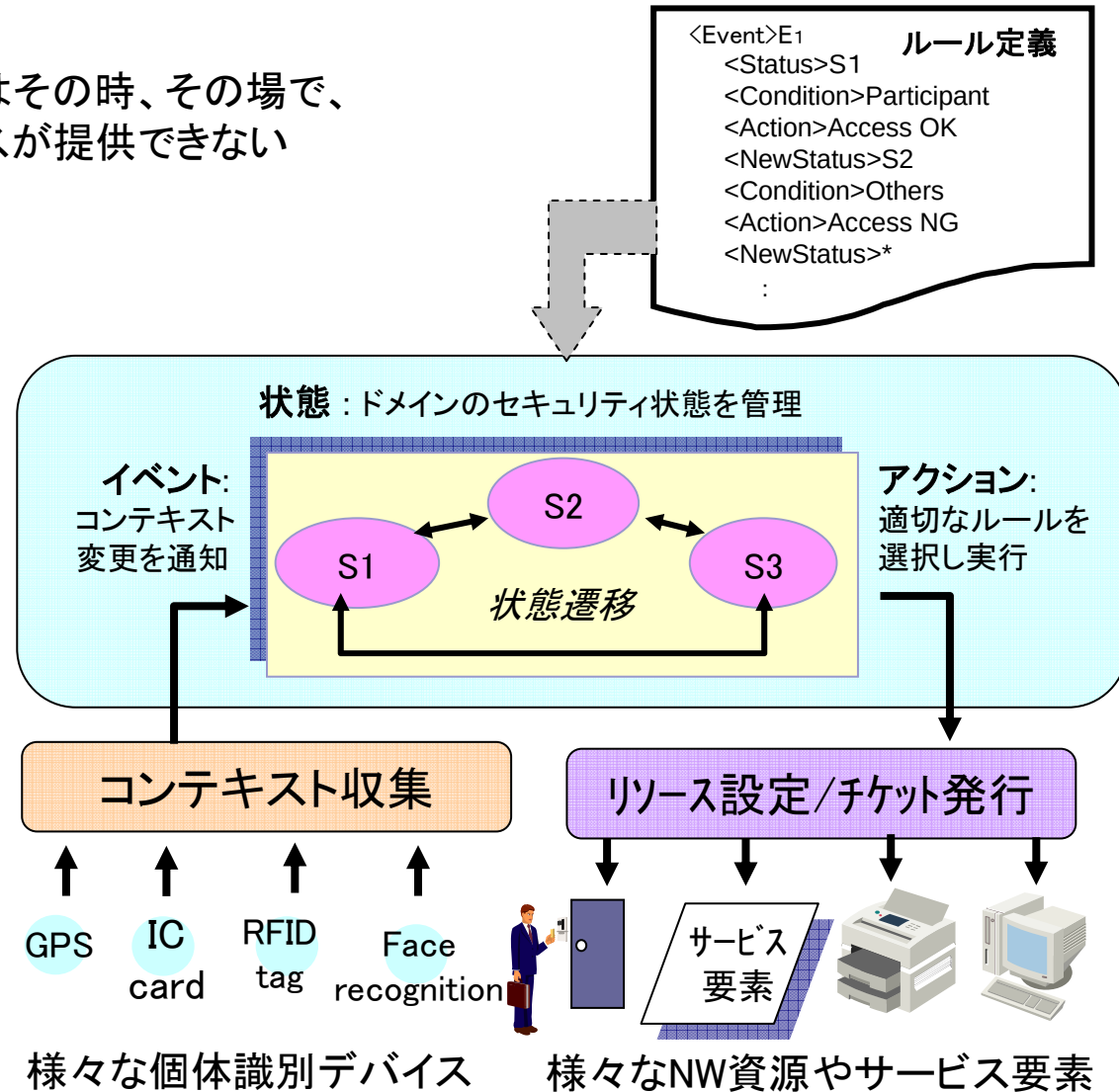


状況適応型アクセス制御

【従来】

- 静的なセキュリティポリシーではその時、その場で、そのユーザに適切なサービスが提供できない

- サービスの認証レベルに応じた多様な認証方法をPlug-in可能
- 利用場所やサービスの状況変化を検出し、ポリシーコントロールを行う
- 電子チケットをユーザ端末やサービスに配布し、ユーザ毎にカスタマイズされたサービスを提供可能



気付きコミュニケーション

【従来】

- ユーザの嗜好や意思をシステムに入力・設定するのが面倒
- PUSH型情報配信では、ユーザが必要以上に大量の情報を受信
- 知り合ったユーザ同士で情報を安全に共有できない

- コンテキストエージェントが実世界でのインタフェースを介し、情報更新やサービス発見を通知
- 商品ブックマークやバディ作りが端末を使った簡単操作で行える
- プロファイル情報へのアクセスや端末操作をユーザポリシーに従って許可する



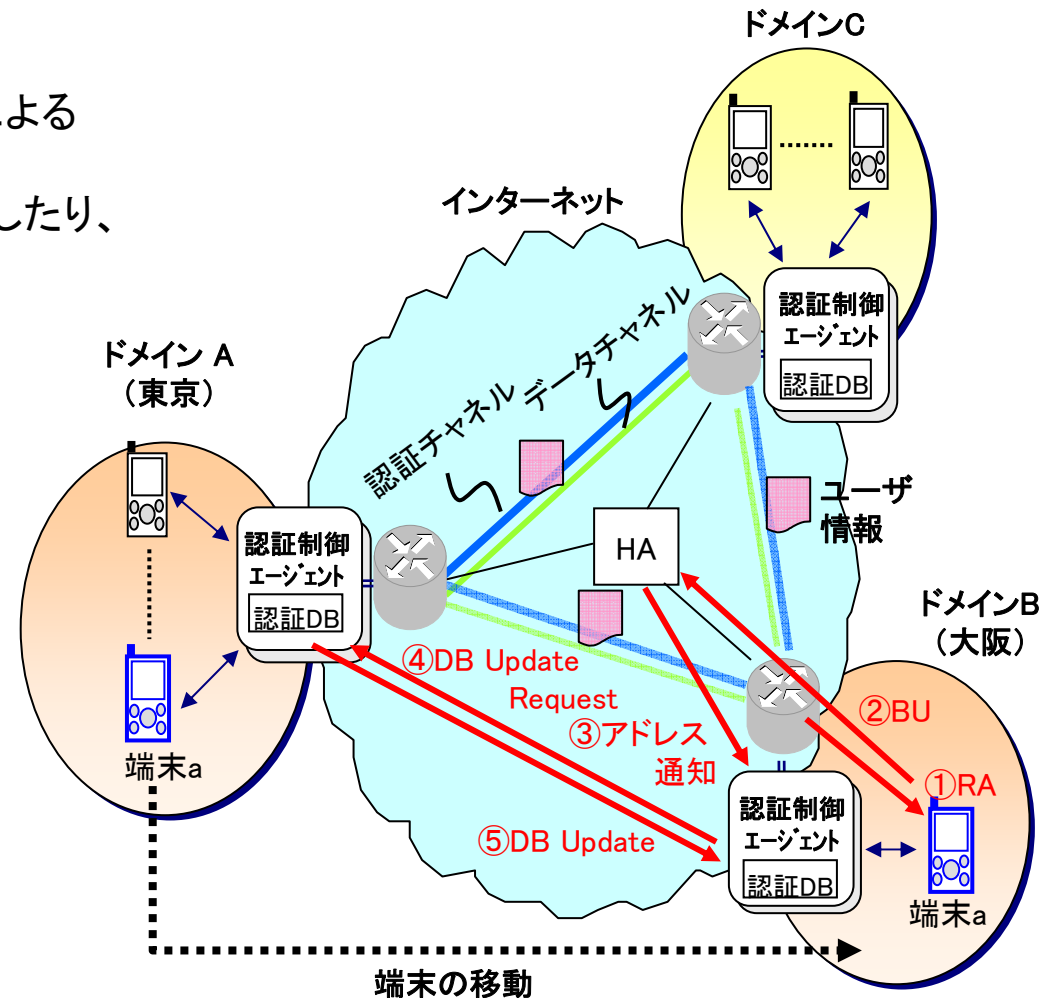
分散認証ネットワーク

【従来】

- 新規端末の追加やネットワーク移動による
端末の参加・離脱に伴って、
認証DBの登録内容に不一致が発生したり、
移動先ドメインで再登録が必要
- サービスを利用する毎、ネットワーク
を移動する毎に認証が必要

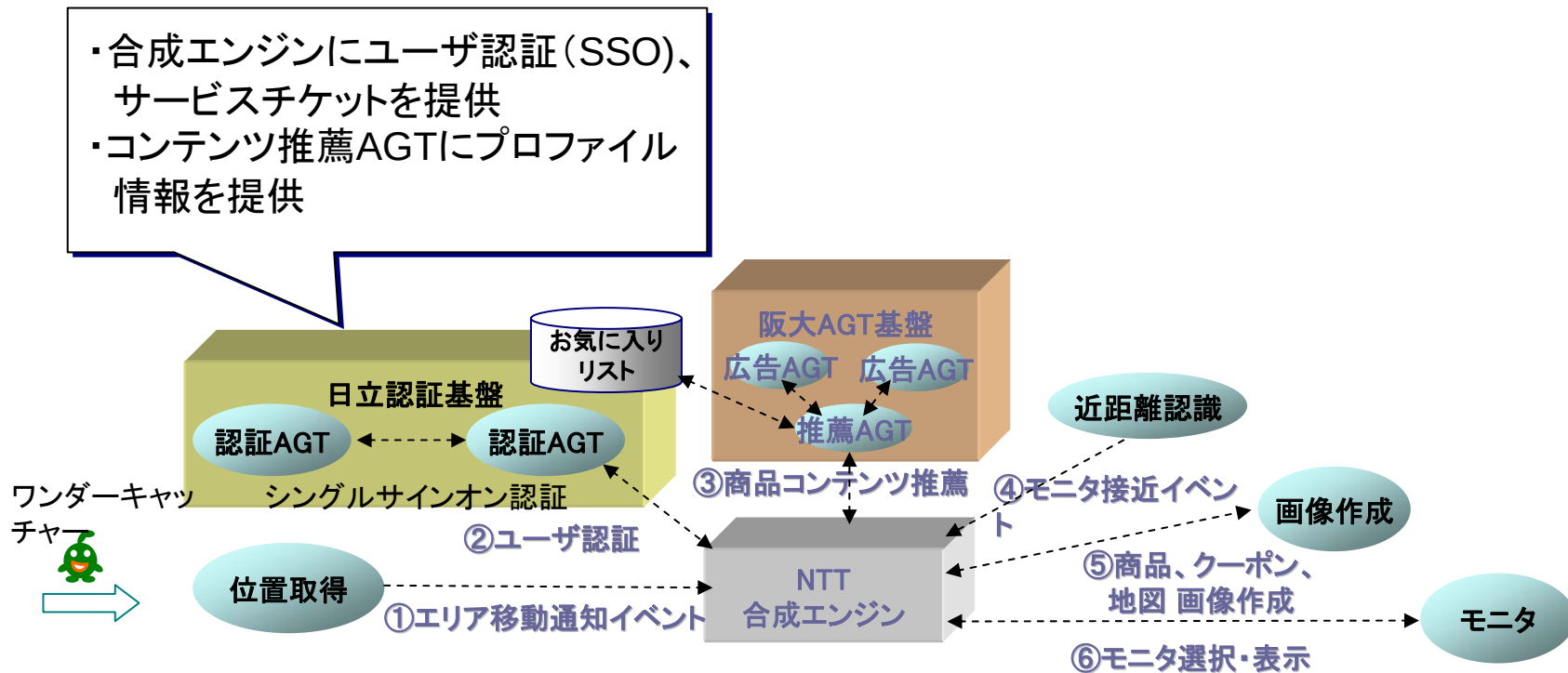


- 認証チャンネルとユーザチャンネル
を分離し、エージェント間の
高速通信を確保
- mobile IPv6 のBinding Update
メッセージをトリガーにして、
ユーザ情報を取得
- エージェント間でユーザ情報を共有
し、シングルサインオンを実現



UNS2005成果デモ

- ショッピングモールにおけるユーザ行動支援システム
 - ワンダーキャッチャ: お気に入り商品ブックマーク、コンテンツ推薦アウェアネス
 - ワンダーシェア : 実世界指向バディリスト形成、プロフィール共有
 - 今どこサービス : 位置ナビ、グループコミュニケーション

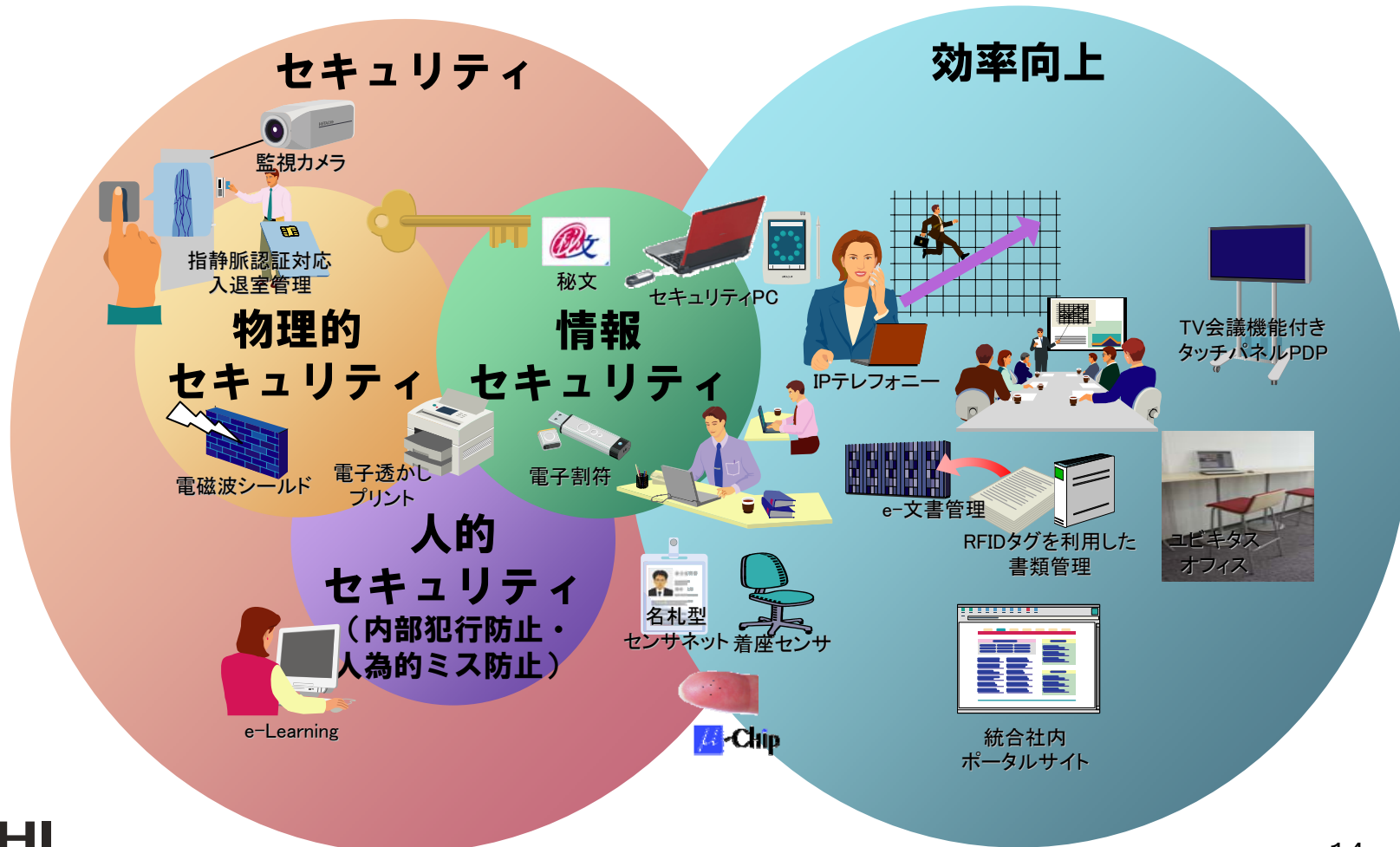


展開例：ユビキタスなワークプレイス



Ubiquitous
Authentication &
Agent

- ・人が合わせていたセキュリティから、人の行動に合わせた動的・柔軟なセキュリティへ
- ・センサとセキュリティ機器が連携し、ゾーン毎に適切なセキュリティレベルを確保
- ・オフィスや従業員のプレゼンスを把握し、効率的なコミュニケーション環境を実現



今後の取り組み

H17年度

- ・シングルプロバイダ
- ・ドメイン独立
(ゾーン間連携)
- ・同種ネットワーク

駅・空港・商業施設・
ショッピングモール等
エリア限定サービス
10～100万ユーザ規模

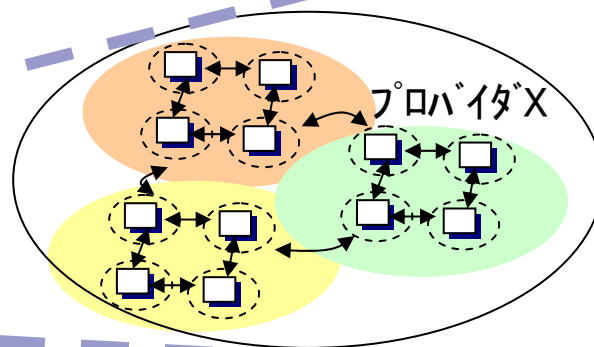


特定エリア/スポット

H18年度

- ・シングルプロバイダ
- ・マルチドメイン連携
- ・異種ネットワーク連携
(無線LAN⇔移動体)

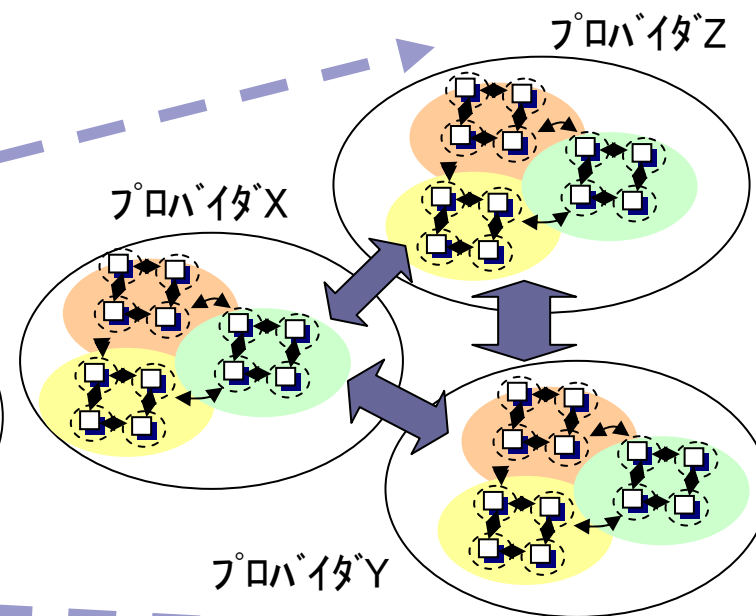
広域ネットワーク
仮想／実空間融合サービス
100～1000万ユーザ規模



H19年度以降

- ・マルチプロバイダ連携
- ・マルチドメイン連携
- ・固定移動網融合(FMC)

全国レベル
ローミングサービス
1～10億ユーザ規模



【補足】 SAML (Security Assertion Markup Language) = ネットワーク認証連携のためのOASIS標準



- 認証・属性・認可情報を安全に交換するためのXMLベースのフレームワーク
Liberty AllianceやGGFでも採用されている
- 何故SAMLか？
 - ① 認証プロトコルや認証デバイスに依存していない → マルチモーダル対応
 - ② データ形式(スキーマ)や転送方法(バインディング)拡張容易 → コンテキスト対応
- 現状のSAMLはWeb-SSOにしか利用されていない
→ SAMLの *Best Current Practice* を作る必要がある
 - ① ネットワーク認証・認可に適用 (802.1x, SIP, MIP, xxx)
 - ② 属性・認可アサーションを用いた、コンテキスト共有やアクセス制御に適用
- ユビキタスサービスへのSAML適用
 - ① セキュアなコンテキスト情報利用 → タイムチケット、ロケーションチケット、アドレスチケット、サービス利用権利チケット等を発行する柔軟な機構
 - ② コンテキスト情報の発見・伝達
→ RFID情報、位置情報を用いて効率的なP2P型検索を可能とする機構