M-138

ユビキタスサービス基盤 (7)
～ユビキタス・オフィス・サービス～

A Ubiquitous Service Platform (7)
- An Application of the Ubiquitous Service Platform -

野田 潤† 中尾 敏康† 柏谷 篤† 谷 幹也† 山田 敬嗣†
Jun NODA Toshiyasu NAKAO Atsushi KASHITANI Mikiya TANI Keiji YAMADA

1. はじめに

多様な情報端末がネットワークで接続され，生活に密着した情報サービスを提供するユビキタス環境が社会に浸透しつつある．近い将来，誰もがいつでもどこでもネットワーク接続することによって，目的や用途に応じたコンテンツにアクセス可能なサービスが実現可能となる．ユビキタス環境において安全で便利なサービスを実現するために，我々が提案しているユビキタスサービス基盤[1]では，暗号技術や，デジタル署名技術，センシング技術を応用し，多様化する端末間で交換される情報の流通管理やアクセス制御を実現する．

本報告では, ユビキタスサービス基盤を用いた, 無線 LAN 環境における情報共有（ユビキタス･オフィス･サービス）を提案する．本サービスは，無線 LAN に接続する不特定多数の端末の中から，適切な環境に存在し，かつ，適切な権利/権限を持つ利用者のみが，安全に情報共有を行える点を特徴とする．

2. ユビキタス・オフィス・サービス

オフィスでは，スケジュールや業務文書などの情報共有が，生産性の観点で重要となる．このような情報共有は，現在，社内イントラネットなどクローズドなネットワークで活用されている．

駅の構内やホテルのロビーなど公共の場所に設置された無線 LAN による接続サービスが始まっている．このような公衆無線サービスは，不特定多数の利用者向けに提供されており，誰もが参加できるオープン性を持つ．公衆無線サービスが増えてくると，外出先でもオフィスにいるのと同様に仕事をするために情報共有を図りたいという欲求が生じると考えられる．

しかし，公衆無線サービスでの情報共有では，無線通信は物理的にオープンであり誰もが傍受できるため，望まない第三者に個人情報や企業情報などが意図せず漏洩してしまうという問題が発生する．

我々はこの問題の解決方法として，次の 2 点を実現することが必要であると考える．

- 利用者/端末の位置や場所等の周辺環境に応じたネットワークへの接続制御
- 利用者/端末に付随するプロファイルに基づく情報へのアクセス制御

周辺環境に応じたネットワークへの接続制御とは，特定の環境に存在する端末に限定してネットワーク接続を許可する制御である．例えば，ある会議室内に存在する端末にのみ接続を許可し，会議室外に存在する端末には許可しないなど端末の外的要因に基づいた接続制御である．

プロファイルに基づく情報へのアクセス制御とは，同じネットワークに接続する不特定多数の端末間で流通する情報へのアクセス制御である．特別な権利/権限をもつ利用者にのみ参照を許可するなど，端末の内的要因に基づいた制御である．

表 1 は，上記 2 点の組み合わせで実現可能な情報共有形態を示す．ユビキタス・オフィス・サービスは，上記 2 点を共に実現することで，オープンなユビキタス環境での安全な情報共有を実現する(表 1-ⅰ).

表 1　公衆無線サービスにおける情報共有形態

		ネットワークへの接続制御	
		有	無
情報へのアクセス制御	有	➢クローズドな通信 ➢グループ向け秘匿通信 (試作サービス形態) (ⅰ)	➢オープンな通信 ➢グループ向け秘匿通信 (ⅱ)
	無	➢クローズドな通信 ➢不特定多数向け通信 (ⅲ)	➢オープンな通信 ➢不特定多数向け通信 (既存サービス形態) (ⅳ)

3. ユビキタスサービス基盤の適用

ユビキタス・オフィス・サービスの実現のために，ユビキタスサービス基盤の備える以下の機構を応用する．

3.1. コンテキスト適応セッション制御機構[2]

本機構は，各端末のセンサで検知した端末の状況（コンテキスト）に応じて，端末の接続可否を判断し，ネットワークセッションの確立/破棄を制御する．センサとしては，赤外光，微弱無線，音声信号などの外的要因を利用する．このセンサにより得られる「サービスエリア内にいる」，「3m 以内の距離で隣接している」などをコンテキストとして，利用する．

3.2. 情報保護流通機構[3]

本機構は，流通する情報を適切な利用者にのみ公開するアクセス制御を実現する．このアクセス制御のために，他端末の探索と発見した端末とのグループ形成，利用者が秘密に管理する個人情報を信頼の基にした端末間の Peer-to-Peer(P2P)認証，グループ内秘匿通信のための通信暗号鍵共有/更新を行なう仕組みを備えている．この機構を用いることで，動的に形成するグループ内で共有される情報は，グループ外へ漏洩しない．

†NEC インターネットシステム研究所，Internet Systems Research Laboratories， NEC Corporation

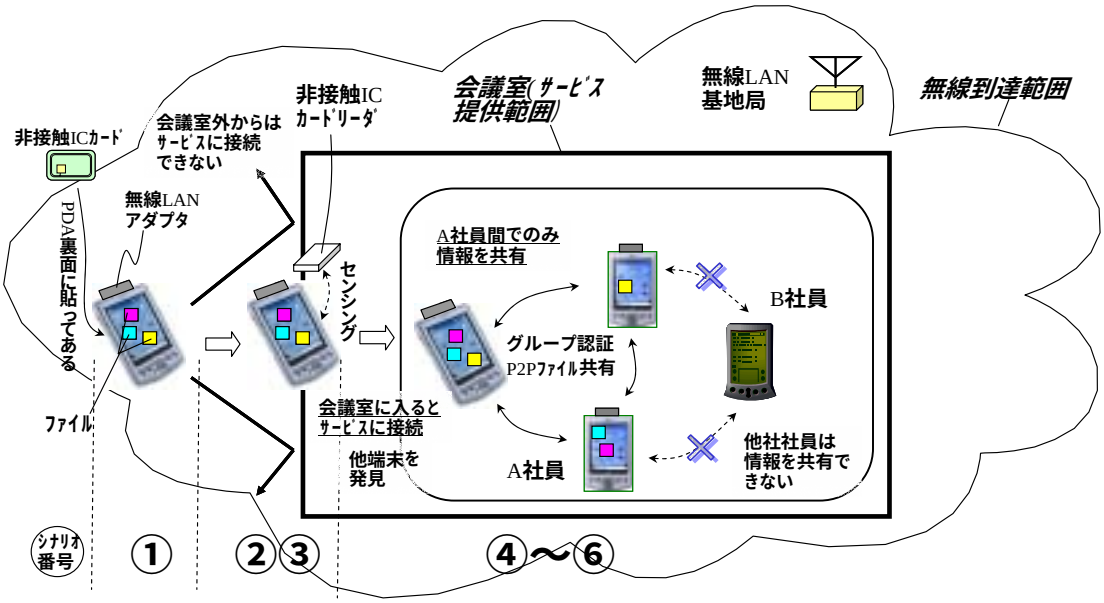

図 1　ユビキタス・オフィス・サービス

4. 試作

3 節で述べたユビキタスサービス基盤の 2 つの機構を用いて，ユビキタス・オフィス・サービスを試作した．

本サービスは，複数企業の社員が参加する合同会議での利用を想定している．各社員の端末にはプロファイル（所属，目的等）が格納されている．また，会議室には，無線 LAN 基地局が設置されている．この状況において，秘匿性が高く，利便性を兼ね備えた情報共有を行う．この情報共有のために，1)会議室内で発信，交換される情報は，会議室外には漏洩しない，2)社外秘情報は，会議室内外を問わず直接関係しない第三者に漏洩しない，3)ネットワークへの接続やコンタクトをとる利用者の発見に手間がかからない，を実現している．

図 1 に具体的な本試作サービスの流れを示す．1.～3.でコンテキスト適応セッション制御機構，4.～6.で情報保護流通機構を利用している．

1. 無線 LAN アダプタを備えた端末が会議室(サービス提供エリア)へ進入．端末には，会議参加証を兼ねる非接触 IC カードがバインドされている．
2. 端末を非接触 IC カードリーダにかざし，会議室内に入ったというコンテキストを得る．
3. 会議室内に入ったというコンテキストを利用して，会議室内端末のネットワークへの接続を許可する．
4. 会議室内に存在する他端末を発見する．同時に発見した端末の公開プロフィールを知ることができる．
5. 会議室内のある A 社の社員は，周辺の端末から，同じ A 社員の端末を見つけた場合，発見した A 社社員の端末とグループを形成する．
6. このグループ内では，A 社の社員のみ参照可能な形で情報共有が行なわれる．他社の社員の端末からは情報は参照できない．

5. 考察

従来の公衆無線サービス(表 1-ⅳ)は，無線到達範囲にいる全ての端末が，その中でやり取りされる全ての情報を参照できるため，安全性に問題がある．本試作サービス(表 1-ⅰ)は，無線到達範囲でも会議室内に存在しない端末には，サービスへの接続が許可されないので，会議室内でやり取りされる情報は参照できない．また，会議室内に存在し，サービスに接続できていても，A 社の社員以外の端末は，A 社のグループに加入できないので，A 社の社員で共有される情報を参照できない．このため会議室内にいるA社社員でのみ情報共有が可能であり，秘匿性の高い情報共有が実現できている．これに対し，情報へのアクセス制御だけを実現した場合(表 1-ⅱ)，会議室外の無線到達範囲にいる A 社社員に情報が漏れてしまう．また，ネットワークへの接続制御だけを実現した場合(表 1-ⅲ)，通信は会議室内に限定されるが，A 社の社員だけで情報を共有することはできない．

企業内，特に応接室など他社関係者の訪れる場所に設置される無線 LAN サービスでは，秘匿性と利便性を兼ね備えた情報共有ニーズがあり，試作した表 1-ⅰの形態が適していると考える．

6. おわりに

本報告では，オープンなユビキタス環境における安全な情報共有を実現するユビキタス･オフィス･サービスについて述べ，ユビキタスサービス基盤で試作したサービスについて説明した．ユビキタスサービス基盤の備える機構を利用することで，安全性の高い情報共有サービスを簡単に構築することができる．今後はプリンタやモニタなどのデバイスと連携し，公共の場所における秘匿性を備えた印刷サービスや表示サービスなど，より高度なオフィスサービスへの応用を検討していく．

参考文献

[1] 柏谷他，ユビキタスサービス基盤(1)～ユビキタスネットワーク構成基盤～，第二回 FIT，2003 年 9 月
[2] 中尾他，ユビキタスサービス基盤(2)～ユビキタスネットワーク構成基盤におけるセッション制御～，第二回 FIT，2003 年 9 月
[3] 野田他，セキュア P2P グループコミュニケーション基盤の提案，第一回 FIT，2002 年 9 月