

プライバシー侵害問題を軽減することを重視した メディア空間への携帯電話機アクセスに関する研究

榊原 憲^{†1,†2} 比嘉 邦彦^{†2}

ユーザ自身の勤務状況映像を、ビデオカメラつき PC 端末を用いて送受信し相互に共有するメディア空間システムにおいて、さらに携帯電話機を端末として接続し利用することができるシステムである「e-office Mobile Access」を開発した。メディア空間システムは Threat of Privacy Violation 問題、すなわち「誰かが自分の知らない間に自分の映像を監視し、自分のプライバシーが侵害されているのではないか」という不安が発生しがちであることが問題であり、それが普及の阻害要因とされていた。そこで筆者らは過去の研究において、映像のユーザ間共有に関して厳格な Reciprocity 制御を施し、かつそのことをユーザが実感できるユーザインタフェースを提供するなどの方法により、この問題を回避した。しかし携帯電話機は勤務状況映像を送信することができないため、これを単にメディア空間システムに接続し PC 端末ユーザの映像を閲覧できるようにしたのでは Reciprocity が不均衡となりプライバシー侵害問題が発生する。そこで、携帯電話機からのアクセスを受け入れる場合でもプライバシー侵害問題を軽減させるための新たな手法を検討し、本システムに実装し評価実験を行った。その結果、携帯電話機からのアクセス時に PC 端末ユーザのプライバシー侵害感を軽減できたことを確認した。また評価実験の過程において、メディア空間システムのユーザは映像共有に関し「自身のプライバシーが侵害される恐れ」以上に「自身が他者のプライバシーを侵害する恐れ」をより強く感じている傾向を発見した。

Cellular Phone Access to Media Space without Privacy Violation

KEN SAKAKIBARA^{†1,†2} and KUNIHICO HIGA^{†2}

The authors have developed the “e-office Mobile Access”, a Video-Mediated Media Space for distributed workers of which user terminals can be not only personal computers with the video camera equipped but also the cellular phone with built-in web browser. Past research indicates that a problem of the media space is so called “Threat of Privacy Violation Problem”, that is, a concern about “Someone might observe my working situation via video while I do not know, and my privacy may be violated”, and it was an obstruction factor for the penetration of the media space. Then, the authors averted this problem by the method such as offering the user interface that provides a strict reciprocity control between users and by which users may actually feel its strictness. However, reciprocity becomes disproportionate and the privacy violation problem may again occur if we allow connection of the cellular phone to the media space system, because the cellular phone cannot transmit the working situation image to the system so that the relationship between PC users and cellular phone users becomes not reciprocal. Then, a new technique to reduce the Threat of Privacy Violation problem even when there is an access from the cellular phone was examined and implemented. As a result, it was confirmed that the Threat of Privacy Violation problem was hardly caused in the PC terminal users even when there is an access from the cellular phone. The authors also found out, in the process of the evaluation experiment, that users of the media space are less sensitive about their own privacy is violated by others, but are more sensitive about violating other people’s privacy.

1. はじめに

「メディア空間 (Media Space)」とは映像を媒介とした通信 (Video-Mediated Communication) の分野であり、「遠隔地から利用できる仮想的な会合場所を生成し、その部屋を訪問する人々に対して、他の人

†1 キヤノン電子株式会社キヤノン電子情報セキュリティ研究所
Information Security Laboratory, Canon Electronics Inc.

†2 東京工業大学大学院イノベーションマネジメント研究所
Graduate School of Innovation Management, Tokyo Institute of Technology

と共存する感覚 (Sense of Co-presence) を提供するよう設計されたもの¹⁾と定義される, ネットワーク情報共有空間²⁾である. この「メディア空間」を適用した通信システムを, 筆者らはメディア空間システムと呼ぶ. メディア空間システムはテレビ電話機やテレビ会議システムとは異なり, コミュニケーション要求の有無にかかわらず複数の遠隔地間で双方向の映像通信を常時継続し, たとえば分散事業所で勤務する勤務者のお互いの勤務状況映像 (オフィスで勤務している姿を PC に接続したビデオカメラで撮像したものを) をユーザ間で共有することにより仮想的な場を生成する. 従来研究ではメディア空間の効果として, 遠隔地に分散して所在する業務グループに対し一体感や仲間意識などを提供できることや, その勤務者らに対してインフォーマルなインタラクションや自発的, 偶発的なコミュニケーションの発生を促すことが可能であることが示されているが³⁾, その効果と引き換えに Threat of Privacy Violation (または Threat of Surveillance) 問題 (以下「プライバシー侵害問題」と呼ぶ) が発生しそれが原因となり利用が中断されがちであることも指摘されていた⁴⁾.

一方, 筆者らはかねてより分散オフィス形態による企業経営を可能にする情報システムの研究に従事しており, 地理的分散オフィス環境にいる勤務者間の一体感, 求心力やグループ意識を醸成でき, かつメンバー間のコミュニケーションを活性化できる可能性を持つメディア空間システムに注目している. そこで筆者らは従来研究で指摘されていたプライバシー侵害問題を解決しメディア空間のメリットだけを引き出すためのメカニズムを研究し, それを実装したシステムである「e-office」を過去開発し⁵⁾, 現在, すでに7年間以上に及ぶ長期実証実験を継続中である⁶⁾.

ところで近年, Web ブラウザ内蔵携帯電話機が多く普及するに従って, 筆者らの周囲からは「PC 端末だけではなく, 携帯電話機からアクセスしたい」という要望が多く寄せられるようになった. その要望の主張は主に, 外出, 出張, 長期休暇, 通勤中など様々な理由でオフィスに不在の「e-office」ユーザが, PC がない場所からも利用したいというものである.

「e-office」では e-office サーバを介して PC 端末が撮像した勤務状況映像をつねに送受信しており, またユーザが入力したメッセージ (フォーマルおよびインフォーマルの両コミュニケーション内容を含む) をサーバ内のデータベースに格納している. したがって, サーバが携帯電話機からのアクセスに応答し, それらの映像やメッセージを携帯電話機の Web ブラウザに

送信することに関する技術的困難さは少ない. しかしながら, 筆者らが過去の研究においてメディア空間特有のプライバシー侵害問題に取り組みそれを解消するメカニズムを実現することに苦労した経験から, PC ユーザの勤務状況映像をそのまま携帯電話機ユーザに送信してしまうような接続サービスをなんのプライバシー侵害対策もなしに提供することはとても考えられなかった.

確かに世間では携帯電話機の普及にともない, 映像を携帯電話機に送出し表示させる様々な種類のネットワークサービスが出現している. しかしメディア空間システムにおいてはその基本的なルールである Reciprocity (情報の相互性, 互恵性) と WYSIWIS (What You See is What I See)²⁾を維持できない接続サービスを安易に提供すれば, プライバシー侵害問題が発生し, 使われなくなるのは明らかである. ユビキタス社会の利便性を追求するあまり, 従来の CSCW 研究で得られた知見を軽視し, 人間の基本的かつ心理学的な問題⁷⁾である「プライバシー侵害問題」を発生させるような振舞いをおこすシステムを開発したのでは, ユーザに受け入れられることは不可能と考えられる. これらの状況に鑑み, 筆者らは「メディア空間システムのユーザにプライバシー侵害問題を発生させずに, しかし携帯電話機からも接続でき, PC 端末, 携帯電話機の両ユーザにメディア空間のメリットを享受させることができるシステム」の実現を目指し研究を開始した.

以下, 2章では主な従来研究, 筆者らの過去の取り組みと本研究の目的について述べ, 3章では「e-office Mobile Access」の設計方針とその議論, およびシステム構築について, 4章ではその評価実験と考察について記し, 5章で関連研究について述べ, 6章においてまとめる.

2. 従来研究

2.1 メディア空間システム

メディア空間システムの従来研究として著名なものに Portholes³⁾がある. その実験報告によると, 2事業所にまたがる複数の研究者を Portholes で結び利用調査を行ったところ, 他の勤務者に対してはすぐにはコンタクトできるか否かの可能性やそれに関する今後の見通しについて知ることができる「コミュニティ内アクセス可否情報提供ツール」として有効であったことや, 「他の勤務者との仲間意識がわいてくる」「深夜や休日出勤の場合に他の勤務者も遠隔地で勤務していることを知りはげみになる」など, 心理的な側面を含

むコミュニティ形成支援効果があったことが報告されている。しかしその実用性を長期継続実験を通じて確認する研究である Nynex Portholes⁴⁾ では、実験当初は Portholes と同様、メディア空間の各効果を確認しながらも、テストユーザから「監視されている感覚がある」、「自身のプライバシーを保護する手段がない」、「誰が自分の画像を見ているのか分からない」などの反応があり、それらの解消を目指してシステム改良（映像の明瞭性を下げる、映像の代替としてアクティビティメータを表示する等）を行ったが、結果としてすべてのユーザには受け入れられなかったとの報告がされている。なお、これらの研究では携帯電話機など、勤務状況映像の撮像手段を持たない端末（以下、non-video 端末と呼ぶ）からのアクセスは考慮されていない。

2.2 プライバシ侵害問題を回避できるメディア空間システム「e-office」

筆者らはこれらの従来研究結果を受け、ユーザにプライバシー侵害問題（正確には、プライバシー侵害感問題：実際には侵害されていない場合でも「もしや侵害されているのではないか」という心理的な不安感をユーザに与えることを含む）を生じさせず、前述したメディア空間のメリットだけを享受できるシステムの実現を目指し、「e-office」システム⁵⁾ をかつて開発した。それに際し、「一般の物理オフィス（通常のオフィススペース）において勤務者はお互いの勤務状況映像を共有している（同僚が見える）が、それにもかかわらず自身のプライバシーが侵害されているとは通常感じない。これは勤務者間の視認性がお互いに Reciprocal かつ WYSIWIS の関係、すなわち自分は他人を見られるが他人も自分を見られるという相互関係があり、かつ全員がほぼ同じ情景を見る状態に保たれているからである」との考察を行い、しかし、Portholes や Nynex Portholes などでは、Reciprocal な関係がプライバシー侵害感の強弱に関係することに気づきながらも、ユーザ操作の自由度やシステムのカスタマイズ性も尊重した結果、Reciprocity を強制的に保つメカニズムを積極的に作り出していないことに注目した。

すなわち、従来研究のメディア空間システムでは、自身の PC 画面上に誰の勤務状況映像を配置するかという他の勤務者の選択の問題は各ユーザ自身に行わせており、その結果ユーザ A は画面上にユーザ B を表示しているのにユーザ B はユーザ A を表示していない場合、監視システムと同様にユーザ B の勤務状況映像がユーザ A へ片方向にのみ伝送され、かつユーザ B がその事実気づかない状態がありえていたこと、その結果として各ユーザにとって「自分が見ているユー

ザ以外の誰かが自分を見ているかもしれない」と懸念しうる状況が発生していたこと、そしてこれが従来研究で最後まで解決できなかったプライバシー侵害問題の主な原因であるとの仮説を立てた。そこで「e-office」システムでは「見える、見られるの関係」をユーザが操作できず完全に Reciprocal であり、かつユーザ自身が Reciprocity の厳格な実装を視覚的にも実感できる、プライバシー侵害に関する不安感を生じる隙のないユーザインタフェースを構築することとし、そのために「固定型オフィスメタファ」の概念を導入し、ユーザが操作できない WYSIWIS ユーザインタフェースを実装した。具体的には：

- 同じグループに所属するユーザは原則として必ず同じ画面、同じ他ユーザを見る、
- 画面上における個室オフィス（各ユーザの勤務状況映像とメッセージの組合せである、ユーザ情報を表示する領域）の配置は固定であり、ユーザ操作により移動できない、

などの制約を意図的にシステム制御に加え、さらにその他のプライバシー保護メカニズム（たとえば映像送受信に関する Reciprocity として、自身の勤務状況映像送信をユーザが停止した場合は、他のユーザの勤務状況映像はそのユーザの画面上に表示しないよう制御、など）の機能をあわせて実装した。その結果、実証実験においてプライバシー侵害問題はほとんど報告されず、グループ体感やインフォーマルコミュニケーション促進などメディア空間システムのメリットを地理的に分散する勤務者間に提供できることを確認した。しかし、本システムにおいても、non-video 端末からのアクセスは考慮されていなかった。

2.3 本研究の目的

Portholes や「e-office」のようなビデオカメラつき PC 端末を用いるメディア空間システムは存在するが、non-video 端末である携帯電話機をメディア空間システムに接続して PC 端末からの映像を受信し、そのことによりメディア空間システムの潜在リスクであるプライバシー侵害問題が PC 端末ユーザや携帯電話機ユーザにどの程度生じるかに関する研究はこれまで行われていない。したがってその実験システムを構築し、携帯電話機をアクセスに用いた場合においてもメディア空間のメリットを享受したままプライバシー侵害問題を解消または少なくとも軽減させることができる技術的解決策を発見し、メディア空間技術のユビキタス化の可能性を探ることが本研究の目的である。

3. 「e-office Mobile Access」

3.1 研究方針

本研究の目的を最終的に達成できる状態とは：

- 携帯電話機を利用端末として加えても、プライバシー侵害感が、PC 端末、携帯電話機のいずれを利用するユーザにも発生しない、
- PC 端末、携帯電話機のいずれから接続してもユーザがグループのメンバー意識やグループ体感を感じられ、両端末相互間を含む全ユーザのコミュニケーションが活性化される、

ことである、そこで本研究ではそれを目指とするシステムを設計・実装し、評価実験によりプライバシー侵害問題を解消できているか否か、およびグループ体感等やコミュニケーション活性化への影響について把握する。

3.1.1 全体システム実装方針

「e-office Mobile Access」の開発にあたり、サーバおよび PC 端末用クライアントソフトウェアに関しては、過去開発した「e-office」のシステムプログラムをベースにモバイルアクセス対応とするための改変を加える。さらに携帯電話機サービス部を新規開発し、これらを統合して「e-office Mobile Access サーバ」を構築することとした。図 1 にシステムの全体構成図を示す。

3.1.2 PC 端末接続に関する採用技術

PC 端末との接続については、前述した過去の「e-office」研究で培った知見を活用し、以下の技術を採用する。

[従来開発技術 1] 固定配置型オフィスメタファ：従来の物理オフィスにおける「制約」を積極的に取り入れることを重視したユーザインタフェース。「制約」の例としては、物理オフィスと同様に画面上ではすべてが固定配置であり画面上のユーザの位置はユーザが勝手に変更できないこと、原則としてすべてのユーザが同じグループ全員の勤務状況映像を含む同じ画面を見ること、あるユーザが（休憩などの理由で）プライバシー機能（映像送信を一時的に停止する機能）を使用した場合、そのユーザへの他のユーザからの映像の配信も同時に停止することなどであり、これらにより Reciprocity や WYSIWIS をルールに厳密に従って実装でき、これが PC 端末利用者間のプライバシー侵害問題を解決できることを過去の「e-office」研究で確認している。

[従来開発技術 2] 職制ベースの管理権限レベル：従来の物理オフィスでは通常、デスクのレイアウトは業

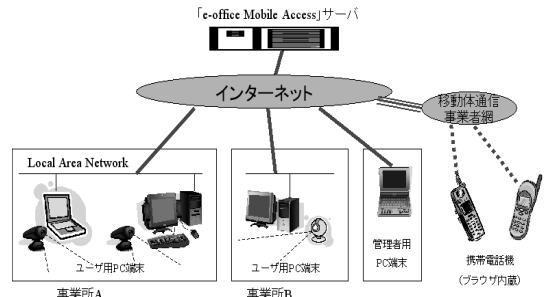


図 1 システム全体構成図
Fig. 1 System overview.

務の内容や役職など職制上の事柄を参考に決定し配置されており、一般勤務者が勝手にこれを変更することは許可されない。その考えに基づき、ユーザの登録、削除、配置させるグループ（仮想的な部門オフィス領域）の選定や、部門オフィス領域中におけるユーザの個室オフィス領域の配置を設定する権限をシステム管理者にのみ持たせ、一般勤務者はこれらをマウス操作等で変更できないよう設計する。これはメディア空間システムを遊びではなく、仮想オフィスとして地理的分散組織等で長期間継続的に利用するために重要なことであることを過去に学んでいる。

[従来開発技術 3] 分散表示・時系列表示混在メッセージング：勤務状況映像の共有に加えて文字情報の共有機能も積極的に取り入れ、これについてはオフィスメタファにこだわらず各ユーザが UI 上から簡単な操作で入力し当該ユーザの映像の近傍に表示し、ユーザ間の情報共有に用いるようにする（分散表示）。なお、チャット形式（時系列表示）も併用する。本機能はユーザ間の様々なコミュニケーションの目的に用いられる。

[従来開発技術 4] メディア空間専用高効率ソフトウェアコーデック：高圧縮時の画質劣化が少ない Wavelet 変換とエントロピー符合化を併用したフレーム内符号化方式のソフトウェアコーデックである。また、人物領域抽出アルゴリズムを内蔵して人物領域を ROI (Region of Interest) としたフレーム内可変量子化制御を行い圧縮率をさらに向上させるとともに人物領域以外のプライバシー侵害問題軽減効果を図っている。

3.1.3 携帯電話機接続に関する設計方針

筆者らが過去の「e-office」研究で開発した上記の [従来開発技術 1]~[従来開発技術 4] に加え、本研究では携帯電話機を接続させるため以下の設計方針をさらに追加する。

[方針 1] 携帯電話機アクセス（以下、モバイルアクセスと呼ぶ）機能を提供しても PC 端末利用者および携帯電話機利用者の双方にプライバシー侵害問題を発生

させず、結果として長期的な利用が可能となるよう設計する。この設計に関しては本研究の基本部分であるため、筆者らを含むシステム開発者間において十分な議論を重ね設計したが、3.1.4 項においてその詳細につき述べる。

[方針 2] メディア空間システムのユーザメリットの維持：プライバシ侵害問題に配慮しながらも、メディア空間システムのメリットであるユーザ間の一体感、グループ意識の醸成やコミュニケーションの活性化を携帯電話機ユーザもできる限り享受できるようにする。

[方針 3] 表示性能、通信料金に関しての配慮：携帯電話機はそのデータ通信速度が高速化しつつあるが、一般の有線ネットワークに比べれば低速な数十から数百 Kbps 程度の通信速度であるため、その環境でもユーザにとって快適な画面表示および操作性が実現できるよう設計する。また、有線インターネット接続は現代では定額制が一般的になったが、携帯電話機の通信料は定額料金制も一部普及しているものの、各種制約があることが多く、当該契約に加入していないユーザも多い。したがって携帯電話機が送受信するデータ量を必要最小限に抑制する必要がある。そこで、その対策として以下の設計とする：

(対策 a) 携帯電話機に表示する勤務状況映像については、e-office サーバから勤務状況映像を継続送信(PC 端末の場合、デフォルトでは 10 秒 1 フレームで継続送信している)するのではなく、携帯電話機からサーバアクセスし、ユーザが表示操作をしたときのみ各ユーザの最新の勤務状況映像をサーバから静止画で受け取る「ワンショット方式」にする。なお静止画のフォーマットは多くの携帯電話機がそのデコーダを内蔵している JPEG 形式とする。なお、JPEG は特許紛争問題が 2002 年に発生したので本システムへの実装に慎重とならざるをえない時期があったが、2006 年 11 月にその問題が収束した⁸⁾ので躊躇せず採用できるようになった。

(対策 b) 対策 a にもかかわらず、あるユーザの在席状況の推移を継続的に知りたいユーザに備えて、画像更新ボタンを携帯電話機の画面上に用意し、その操作により更新して表示させる。

(対策 c) 携帯電話機で表示可能な各種絵文字(各携帯事業者がその規格を定めるビルトインアイコン)は、それと同様の絵文字を GIF 画像等でサーバから伝送する場合に比べてデータ量の大幅な削減が可能であり、携帯電話機での表示速度や使い勝手を向上させ、かつ通信料金低減の効果もあることから、積極的に活用する。ただしそのためには、事業者ごとに異なる文字

コードおよびデザインの絵文字を利用していることから「e-office Mobile Access」のサーバ側において、携帯電話機からのアクセス要求である HTTP Request ヘッダ情報に含まれる HTTP_USER_AGENT の内容を確認し、接続してきた携帯電話機の事業者を UA (User Agent) により識別して、その事業者が定める絵文字コードを送出する処理を実装する。

(対策 d) 機種依存性の軽減：携帯電話機の液晶表示部の解像度やサイズは近年拡大する傾向にあり、また主に JAVA 言語をベースとしたクライアントプログラムを実行可能な携帯電話機も多く存在する。しかし、それらの機能を持たない機種を利用しているユーザも多くいることから「e-office Mobile Access」では、携帯電話機用 Web 画面(いわゆる「携帯サイト」の画面)を表示可能な機種であればほとんどの携帯電話機で表示できるように HTML コードを生成する。具体的には、前述の方法で UA を取得し携帯電話機の事業者を識別し、コンパクト HTML (NTT docomo 社用)、XHTML Basic (KDDI/au 社用)、HTML のサブセット (SoftBank Mobile 社用)の各 HTML コードをそれぞれ生成する。

(対策 e) PC 端末用画面との相違が少ない、違和感のないユーザインタフェース (UI)：本システムでは、同一のユーザが状況(居場所等)により PC 端末または携帯電話機のいずれかから接続することから、どちらの場合でも大きな相違のない UI を実現することを目標とする。また、3.1.2 項に記した PC 端末用 UI 設計は携帯電話機用 UI にもその思想を適用することでプライバシ侵害問題の軽減やインフォーマルコミュニケーションの活性化に寄与することが可能であると思われるので、極力 PC 端末用 UI に準ずる形で実装する。同一グループに関する PC 端末用 UI の画面例を図 2 に、携帯電話機用 UI の画面例を図 3 に示す。

3.1.4 携帯電話機アクセス時のプライバシ侵害問題を軽減させるための議論

これまで PC 端末により「e-office」(モバイルアクセス機能のないもの)の利用経験があるユーザは、ユーザ間がお互いに Reciprocal かつ WYSIWIS な状態であることが(たとえ説明を受けなくても感覚的に)分かっており、プライバシ侵害問題がないことに関してシステムとの信頼関係が築かれている。それはこれまでのアンケート調査結果からも、また利用が長期間にわたり継続していることから実証されているといえる。その背景には、他メンバの誰が現在アクセスしているかをお互いの UI で確認でき、それが事実であることを各メンバが信頼できていることが大きい。し



図 2 PC 端末用 UI 画面 (一部)
Fig. 2 UI Screen for PC.

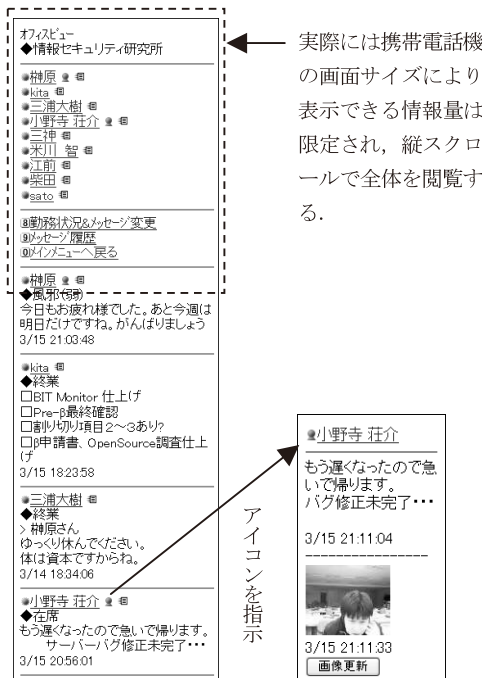


図 3 モバイルアクセス用 UI (一部)
Fig. 3 UI Screen for mobile access.

しかし「e-office」以前の従来研究結果^{3),4)}から、自身の勤務状況映像など PC 端末や携帯電話機の画面に表示されている内容が、たとえ同じグループのメンバからであっても自身が知らない間に閲覧される可能性があるとなつたとたんに、これらの信頼関係は簡単にくずれてしまうことが予想される。そこで、モバイルア

セスに関わるプライバシー侵害問題軽減の基本設計方針に関して、筆者らは従来の e-office 設計関係者を含む合計 5 名の間で Reciprocity, 公平性, 汎用性, ユーザの順応性 (分かりやすさ), 情報システムモラルなどの観点からアイデア出し (仮説の検討) を行った。そして、本来は提案されたアイデアのすべてを実装し評価実験を行うのが望ましいがそれは困難であるため、各アイデアに関して仮想設計による実装工数見積もり、およびプライバシー侵害軽減効果予測の議論を行い、実装が容易かつ大きな効果が期待できそうなものを実装し実証実験を行うことにした。アイデアは大きく分けて以下の 6 種類であったが、それらの内容、意見、およびそれらをもとに議論した結果としての採用・不採用の判断結果について以下に記す。

(ルール案 1) 全員利用可能ルール: PC 端末ユーザの全員が携帯電話機からもモバイルアクセスできる公平なシステムとする。実際には PC 端末から接続するための ID やパスワードと同一のもので携帯電話機から接続するよう実装する。

(ルール案 2) 携帯アクセス頻度制限ルール: ユーザが最も嫌うシナリオは、たとえ上記 (1) のルールがあっても、① PC 端末から接続するユーザ、② 携帯電話機から接続し①のユーザの勤務状況映像を閲覧するだけのユーザ、のように①と②が分離し固定化してしまうことである。そうではなく、通常オフィスで勤務するときは PC 端末から自身の勤務状況映像を送受信するユーザが、外出先等からはモバイルアクセスを許可される、という使われ方である必要がある。その考え方を機能として実装するためには、PC 端末からの接続時間に比例してモバイルアクセスの利用可能時間や回数を制限する等の方法も考えられる。しかし、実際の利用状況として職制や業務内容によりメンバごとに PC 端末接続とモバイルアクセスとの比率が異なることが予想されるため、今回は実装を見送った。

(ルール案 3) 画像提供ルール: 昨今の携帯電話機はカメラ内蔵のものが多いので、オフィスから外出中のユーザは携帯電話機内蔵のカメラで撮影した画像をサーバに送信した場合のみ、引き換えに他ユーザの勤務状況映像を受信できるようにするのが良い、との意見があった。これは画像/映像の Reciprocity を保つというメディア空間の基本に、モバイルアクセスでも忠実に準拠しようとする考えといえる。しかしカメラ内蔵携帯電話機で撮影できる画像は、通常は携帯電話機ユーザの顔や近隣の景色等であり、ユーザの勤務状況映像ではないため、これでは Reciprocity にはなりえず意味がないとの意見が多く、結局不採用とした。

しかし、モバイルユーザが自身の現在の所在場所（たとえば訪問地の様子）の画像を PC 端末ユーザに送信すれば、これは一種のプライバシー情報の公開であり、このプライバシー情報と引き換えに PC 端末ユーザの勤務状況映像を提供することは公平で良いのではないかと意見は、不採用を決定した後も根強く主張された。（ルール案 4）異メディア（画像以外）のプライバシー情報提供ルール：映像送受信の Reciprocity にこだわらず、「プライバシー情報公開の Reciprocity」という考えをとり、PC 端末ユーザが送出する勤務状況映像と引き換えに携帯電話機ユーザもなんらかのプライバシー情報を携帯電話機から提供してはどうか、というアイデアがあった。特に近年 GPS（全地球測位システム）の情報を取得し送信できる携帯電話機があることから、モバイルユーザが携帯電話機でアクセスする際に、ユーザの GPS 位置座標情報をサーバに送信し、サーバではそれをもとに所在地文字情報（たとえば秋葉原、Seoul など）に変換して PC 端末ユーザの画面に提供し、それと引き換えに携帯電話機ユーザは PC 端末ユーザの勤務状況映像を受信できるよう制御してはどうかというものである。モバイルユーザの「居場所」というプライバシー情報と PC 端末ユーザの「映像」という異なる種類のプライバシー情報を交換する考え方であり、種別は異なるがお互いにプライバシーを公開するという公平性の観点から良いという意見があった。また、モバイルアクセスのニーズは「外出中」のメンバが主であることから、その所在地をオフィス内勤中のメンバの PC 端末にも共有して表示することは、「皆がそれぞれの異なる場所で共通の目的のために働いている」という一体感を得るのに有効ではないかという意見もあり、同意者が多かった。しかし携帯電話機が GPS 対応端末に限定され、その普及率がかならずしも高くないことから、本ルールの実装は今回は断念した。（ルール案 5）2重ログインルール：PC 端末からサーバに接続中であるユーザと同一のユーザ（同一の ID およびパスワードを用いる）のモバイルアクセス（2重ログイン）を許可し、逆に PC 端末から接続中でないユーザのモバイルアクセスは拒否する考え方。すなわち、オフィスにおいて PC 端末をサーバに接続したままの状態を外出し携帯電話機によりアクセスしたユーザには、自身の PC 端末からの映像や、他ユーザの勤務状況の映像を送出する。当該ユーザ自身はオフィス外にあり、そのユーザと他ユーザの勤務状況映像に関する Reciprocity が保たれるわけではないので、意味がないという意見もあり、結果として、プライバシー侵害問題軽減策としては有効ではないと判断された。し

かし、PC 端末からオフィスでの不在情報を提供しているから人ではなく場所の状況情報を共有するという面では Reciprocal ではないかとの意見もあり、結局本ルールはプライバシー侵害問題の軽減策としては認められなかったものの、前記の形での 2 重ログインは許可するよう実装することにした。したがって実装後は、自身の PC 端末でログインしたまま外出し、モバイルアクセスするユーザも多少見られた。運用開始後その効果として、「他の PC 端末ユーザには、たとえ人が映っていない勤務状況映像であっても、やはりメンバのデスク近辺の映像が閲覧できると、特にそれが遠隔地であった場合、場や時間の一体感が保たれるので、PC 端末もログアウトしてしまうよりは良い」との意見があった。

（ルール案 6）被閲覧事実通知ルール：モバイルアクセスがあった場合、その事実を PC 端末ユーザに即座に知らせるルール。すなわち、メディア空間システムにとって重要な Reciprocity が一時的に崩れ、監視されている状態となっていることを PC 端末ユーザに知らせ、各ユーザの好みに応じた対応をとらせ、プライバシー侵害感を軽減する考えである。周知する方法としては、PC 画面にモバイルアクセス通知画面をポップアップ表示（モバイルアクセスユーザの名前とアクセス時刻を表示）し、かつ PC のスピーカより警告音を鳴動する（ユーザが動作を選択可能だが、初期設定は双方をオンとする。なお、その設定画面を図 4 に示す）。これにより、PC 端末利用中またはその近くにいるユーザはモバイルアクセスに気づくことができ、non-Reciprocity 状態にあることを知り必要に応じてプライバシー侵害問題の対応（携帯電話機から監視されることを好まない場合には、映像送受信を OFF にする、自身のメッセージを書き換える等）をとることができるので、これを採用することとした。またこの機能が実装されることにより、携帯電話機ユーザはアクセスした事実が PC 端末ユーザに知られることになり、携帯電話機ユーザにはそのこと（いわば、覗いているこ

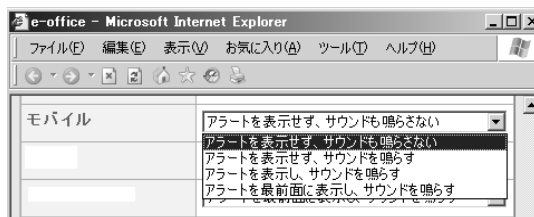


図 4 モバイルアクセス通知機能の設定画面

Fig. 4 User screen to choose mobile access notification method.

表 1 プライバシー侵害問題軽減ルール案一覧と実装

Table 1 Privacy rule plans and implementations.

プライバシー侵害問題軽減策案	議論 (有効か)	今回実装
(1) 全員利用可能ルール	有効	実装する
(2) アクセス頻度制限ルール	有効だが運用困難	—
(3) 画像提供ルール	有効, 無効両論あり	—
(4) 位置情報提供ルール	有効だが端末限定	—
(5) 2重ログインルール	無効?だが弊害なし	実装する
(6) 被閲覧事実通知ルール	有効	実装する

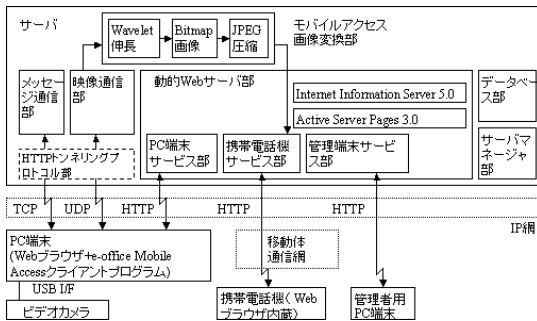


図 5 全体システム構成

Fig. 5 System architecture.

と)に関するプライバシー公開義務が発生することから, それを嫌う携帯電話機ユーザからの無駄なモバイルアクセスが減り, その結果 PC 端末ユーザのプライバシー侵害問題も減少するのではないかとの意見があった.

このような議論を通じてプライバシー保護機能のアイデア出しを行った結果, 「e-office Mobile Access」の基本的なプライバシー侵害問題軽減メカニズムとして, ルール案 1 とルール案 6 を採用することにした. ルール案 5 については前述のように消極的にだが実装した(表 1).

3.2 システム構成

図 5 に全体システム構成を示す. これに示されるように, ユーザ PC 端末, 携帯電話機, 管理者用 PC 端末は, 同一サーバの動的 Web サーバ部に接続するが, 接続時に異なる URL を指定することによりそれぞれのユーザサービスを受けることができるように構成した. なお携帯電話機ユーザがサーバにアクセスした際には前述のモバイルアクセス通知機能により, モバイルアクセスがあり一時的に Reciprocity が崩れている旨の通知がユーザ PC 端末に図 6 に示す画面によりなされる. その後, 携帯電話機の Web ブラウザには図 3 に例を示した画面 (モバイルアクセス用オフィスビュー) が送信される.

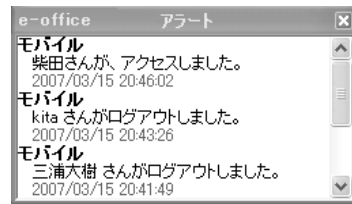


図 6 モバイルアクセス通知機能画面

Fig. 6 Pop-up message of mobile access notification function.

3.3 携帯電話機用ユーザインタフェース実装上の問題点と実際

3.3.1 1 ページのデータ容量制限

前述の設計方針に基づく実装に際し, 技術的に特に苦勞した点を参考のため以下に記す. PC 画面の UI と携帯電話機の UI とは極力似た構成にすることを目標としたので, 筆者らは当初携帯電話機のオフィスビュー画面には PC 端末と同様, ユーザ自身と同じオフィス (グループ) に所属する他ユーザの氏名, ログイン状態, 勤務状況 (在席, 休憩, 外出, 終業などからユーザが選択. これらの選択肢はシステム管理者のみがサーバに設定登録できることにより, 遊び的な使い方を防止している. なお選択はユーザが行う), メッセージ (自由文章) に加えて個人の勤務状況映像を 1 個の仮想的な個室オフィスとして表示し, それをメンバの人数分 (最大 20 人) 縦に並べた画面を生成して送信, 表示させようとした. これにより PC 端末ユーザと携帯電話機ユーザとの間の WYSIWIS 性が強まり, また携帯電話機ユーザも縦スクロールだけで自分が所属するオフィス全体の状況が分かるので使いやすさの面も向上することを期待した.

しかし実装過程でそれが技術的に困難であることが分かった. 携帯電話機のブラウザの多くは 1 ページあたりトータルの最大データサイズが 8 Kbytes 程度の制限となっているものが多く, サーバからそれを超えたデータ量を送信すると, ページエラーを起こしてしまう. しかし「e-office Mobile Access」サーバが送信する JPEG 画像はその解像度は小さいが判別可能にするためには平均でも 1 枚あたり 2 Kbytes 程度は必要であり, したがって, PC 端末ユーザが 10 人いるオフィスでこれを表示するためには, 約 20 Kbytes なので, エラーになってしまう. 最近のいわゆる「フルブラウザ携帯」などであれば表示はできるが, それに限定するのは前述の携帯電話機接続に関する設計方針, 3.1.3 項の (対策 d) で策定した「機種依存性の軽減」に反する.

携帯電話機にオフィス全員の勤務状況画像を同時に

表示し、PC 端末 UI との WYSIWIS 性を保つことは開発者の念願だったので非常に残念ではあったが、上記の事情を考慮してやむをえず基本画面には JPEG 化した勤務状況映像を含めず、ユーザごとに「画像あり」アイコン（図 3 左側画面のユーザ名の右にある図形）のみを表示し、携帯電話機ユーザがこれを指示したときにその 1 人のみの画像を表示する別画面（図 3 右側の画面）に推移する仕様とした。

3.3.2 絵文字の問題

そのほかに苦労した点として、絵文字の問題がある。3.1.3 項の（対策 c）で説明したように、携帯電話機向けネットワークサービスで絵文字を使う場合、携帯電話機のビルトインアイコンを利用するメリットは大きい。そこで、本システムでも当初よりその方針ではあったが、一方で今後の新規携帯事業者や新規端末（User Agent の定義が現時点では不明な端末）等からのアクセスに備えて、まず本システムに必要な合計 24 個のカラー絵文字アイコンを GIF ファイルとして制作した。制作した 12×12 pixels の GIF ファイルアイコンは 1 個あたり約 100 byte から 300 byte のデータ量があったので、たとえばモバイルアクセス用オフィスビュー 1 画面では最大 13 個の GIF ファイル使用により（勤務状況映像用 JPEG ファイルがなくても）合計で 3Kbyte 程度のページサイズになっている。しかし前述した方法によりサーバで User Agent を取得し、携帯電話事業者が判明した携帯電話機に対しては、事業者が定める類似したデザインのビルトインアイコンのコード（通常 4 バイト）にサーバで置換することにより、データ量を大幅（画像だけで約 25 分の 1 から 75 分の 1）に圧縮することができ、操作性も向上する。そのために、各携帯電話事業者が定めるビルトインアイコンの中から本システムの GIF ファイルアイコンに類似したデザインのものを選択し対照関係をデータベースに保存して携帯用画面生成時に置換している（なお、ビルトインアイコンの絵柄に関しては著作権の問題でここでは図示しない）。

しかしここで困ったのは、ビルトインアイコンに、e-office Mobile Access で使用したい性格の絵文字（図 7）がない場合があるという問題であった。携帯電話機が備えるビルトインアイコンは主としてパーソナルコミュニケーションに用いることを想定しているためか、グループウェア的な概念を示す絵文字はあまり充実していないようである。特に図 7 に示す概念および画像と似たものを持つ事業者はないか少なかった。そこで、たとえば「オフライン状態」に“zzz”という絵のビルトインアイコンを利用したが、これを用いるとそ

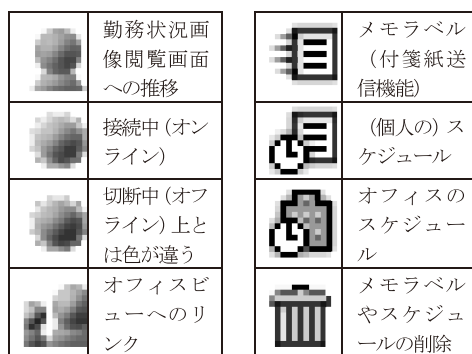


図 7 携帯電話機に類似アイコンがない絵文字の例

Fig. 7 Pictograph not available for the cellular phone.

のデザインおよび着色とも（ビジネス用途である仮想オフィスシステムの UI としては）多少ふざけた印象になってしまうという問題が残った。

3.3.3 複数の同時モバイルアクセスへの対応

本システムは PC 端末ユーザをユーザの主体とした考えであり、かつ 1 オフィス（グループ）あたりのユーザ数が最大 20 人で複数のモバイルアクセスが同時発生する頻度は低いと考えられることから、もしそれが発生した場合のモバイルアクセスユーザ同士の通知方法等についての工夫は取り入れないよう割り切ることとした。モバイルアクセスユーザはあくまで図 3 の形式の画面を閲覧でき、もし 2 人のユーザが同時にモバイルアクセスしているとしても、その事實は 2 人のどちらも気づかないことになる。しかし将来モバイル利用を主体としたメディア空間システムを検討する場合には改善する余地を残した。

4. 評価実験と考察

4.1 評価実験 1（プライバシー問題軽減機能の評価）

ここでは、前記議論に基づくプライバシー侵害問題軽減メカニズム（ルール案 1）（ルール案 5）および（ルール案 6）を実装した効果を評価する。その評価実験の被験者を定めるにあたり、本システムの開発者は後述する問題（プライバシー侵害感に関し一般人とは違う感覚を持つ可能性）があり正しく評価できないことも予想されるので、本評価実験の被験者をメディア空間を初めて利用する者としてすることとし、2006 年 9 月 1 日に 9 人で構成される仮想オフィスを設定した。この仮想オフィスのメンバ 9 人のうち 1 人は管理職でかつ本システムの詳細を熟知しているが、残りの 8 人は一般職のソフトウェア技術者で、全員にとり「e-office Mobile Access」が初めて利用するメディア空間システムであるので、この 8 人を被験者とする（グループ

A と呼ぶ) . 8 人のうち 7 人は同一事業所に勤務, 他の 1 人は地方の大学院研究室で 7 人の業務と関連する産学共同研究に従事している .

この期間, 不公平であることを承知で 1 人の管理職のみが PC 端末に加えてモバイルアクセスを利用し, 同じ仮想オフィスのメンバであるグループ A の 8 人の被験者には PC 端末のみを利用させ (被験者はシステムにモバイルアクセス機能があること, 管理職がそれを行うことは知らされているが, アクセス方法は知らされていないので自身では使えない), 被閲覧事実通知ルールに基づくモバイルアクセス通知機能 (図 6) をシステムの停止し管理者がモバイルアクセスするタイミングや頻度を被験者に気づかれない状態にした (つまり被験者は自分の映像がいつ閲覧されているのか, 分からない状態) . その後 9 人のユーザは就業時間中に PC 端末よりほぼ毎日ログインし利用していたが, 約 6 カ月が経過した 2007 年 2 月に (ここまでを第 1 期間とする), 被験者 8 人に対しアンケート調査を実施し, 勤務状況映像, オンライン状態, メッセージの 3 つの項目それぞれに関し, 管理職 1 人が携帯電話機から被験者の気づかない間に閲覧していることに関しどの程度のプライバシー侵害感を感じるかについて, 「強く感じる」, 「少し感じる」, 「あまり感じない」, 「まったく感じない」の 4 段階の質問を行い, これらに 4 点 ~ 1 点をそれぞれ与え各項目ごとの平均得点を求めた .

次に, アンケート調査回収後ただちにモバイルアクセス通知機能を利用可能とし, かつ被験者全員に携帯電話機からのモバイルアクセス方法 (URL 等) を知らせ次の評価期間 (第 2 期間) に移った . ここでは各被験者も自らの携帯電話機によるモバイルアクセスを体験し, また PC 端末の画面に表示されるモバイルアクセス通知機能を実際に経験した . 第 2 期間開始の 2 週間後に, 前回とまったく同一内容の質問のアンケート調査を再度実施し得点を求めた . その結果を, 第 1 期間と第 2 期間の比較として表 2 に示す .

第 1 期間と第 2 期間の差を確認するため t 検定を行ったところ, 特に勤務状況映像 (を閲覧されること) については有意差があり ($T(14)=2.74, P=0.007<0.05$), また, メッセージについても有意傾向を認めた ($T(14)=1.66, P=0.059<0.10$) . これにより, 実装したプライバシー問題軽減機能は少なくとも勤務状況映像とメッセージについては有効であったといえる .

一方, オンライン状態 (を閲覧されること) については統計的有意差は認められなかった . 実験中の観察によるその理由の考察としては, 第 2 期間にはモバ

表 2 プライバシ侵害感 (グループ A)
Table 2 Privacy invasion feeling of group A.

	第一期間	第二期間	期間単純平均
勤務状況映像	2.625	1.125	1.875
オンライン状態	2.125	1.750	1.938
メッセージ	1.750	1.250	1.500
上記メディア平均	2.167	1.375	1.771

イルアクセス通知機能によりアクセスが頻繁にあることを被験者が知った場合, 被験者の顔がカメラに映らないようにカメラの向きを肩, 腕などに変える, メッセージは消去する (チャット形式画面には残る) という対応が可能で実際にそれをする被験者もいたが, これに対し, オンライン状態は PC 端末がシステムに接続している限り強制的に携帯電話機の画面に表示され閲覧者から確実に把握されるので, 比較的プライバシー侵害感が残り第 1 期間との際が少ないものと推測される (被験者全員は本システムの PC 端末を, 他の PC アプリケーションを動作させる PC と共用しており, 他メンバからの有用なメッセージも閲覧できるなど本システムのメリットを享受するため, オフラインにすることは少ない) . なお, 第 1 期間から第 2 期間に移行する際にルール (1), (5) および (6) を同時に適用したため, その 3 つの効果の影響度は測定できていない .

4.2 評価実験 2 (プライバシー問題軽減機能の, 被験者の違いによる影響評価)

評価実験 1 において, 本システムの開発者は被験者としてふさわしくないと述べ, 被験者を初めてメディア空間システムを利用するグループ A の 8 人とした .

そのこと自体の検証, すなわちメディア空間初心者であるグループ A と, 本システムをよく理解している被験者 (長期利用者) との差異を評価するため, サーバにグループ A とはまったく独立した仮想オフィスであり 8 人で構成されるユーザグループ B を設定し, 2006 年 9 月 4 日より実験を開始した . 本グループ 8 人のうち 4 人は本システムの設計または実装に関わっており, それ以外の 4 人もモバイルアクセス機能のない過去の「e-office」から「引越し」してきた者で, 評価実験の開始時点からモバイルアクセスの存在と利用方法の説明を受けている . そのため, 実験開始当初から PC 端末からのアクセスおよび携帯電話機からのモバイルアクセスの双方を使用し, モバイルアクセス通知機能が設定可能であること (図 4 に示す通知方法の選択) に関してもその存在を知っており, 初期設定

表 3 プライバシ侵害感比較 (グループ A と B)

Table 3 Privacy invasion feeling comparison of group A, B.

	グループ A 第 2 期間	グループ B 全期間
勤務状況映像	1. 125	1. 833
オンライン状態	1. 750	1. 167
メッセージ	1. 250	1. 500
上記メディア平均	1. 375	1. 500

(モバイルアクセス通知画面の最前面ウインドウ表示, サウンド鳴動)とは異なる設定に変更する者もいた.

6 カ月後の 2007 年 2 月にグループ B の被験者にグループ A に対して行ったものと同じの質問のアンケート調査を行ったところ, うち 6 人より回答を得たので, 前述と同様の方法で得点を求めた. その結果を表 3 の右側に示す.

グループ A の第 2 期間とグループ B とを比較すると, 勤務状況映像に関しては, むしろグループ B の方がプライバシ侵害感が強く, グループ A の第 2 期間に対する有意差も認められた ($T(12) = -3.48, P = 0.002 < 0.05$). また, オンライン状態は評価実験 1 (グループ A の第 1 期間と第 2 期間の差) よりは差が大きくほぼ有意傾向にあり ($T(12) = 1.30, P = 0.109$), メッセージ閲覧については有意差は認められなかった.

グループ B がグループ A の第 2 期間に比べて, 映像についてプライバシ侵害感が強いことの原因は不明だが, アンケート調査後のヒアリング調査により筆者らが得た感触に基づく推測としては, グループ B の被験者は本システムの研究者・設計者を含むためメディア空間システムのプライバシ侵害に関する問題意識が高く, 勤務状況映像の被閲覧に慣れていてもアンケート調査時は自然と高い点数をつけたものと推測する. 逆にオンライン状態に関するプライバシ侵害感が低い理由としては, 前述のように 2 重ログインを行うため不在でも PC 端末をログインし続けている被験者がおり, その場合オンライン状態の表示内容自体に意味がないこと, グループ B の各ユーザは映像で在席状態を知ること慣れていて, オンライン状態の情報は注視していないことが原因であった可能性が高い.

4.3 評価実験 3 (モバイルアクセス通知機能の機能評価)

前述のように, プライバシ侵害問題軽減策案 (6) である被閲覧事実通知ルールを, モバイルアクセス通知機能として本システムに実装し, 図 4 に示す 4 種類の設定をユーザが選択可能とした. そこで, その機能,

表 4 モバイルアクセス通知機能設定と他の回答とのクロス分析
Table 4 Cross table between setting of mobile access notification function and other evaluation.

モバイルアクセス通知機能の設定状況に関する質問への回答		設定 A	設定 B	設定 C	設定 D
(各設定の意味)	画面アラート サウンド鳴動	最前面 有	有 有	無 有	無 無
質問: 他ユーザがモバイルアクセスした時に, 自分がそれに気づいていると思うか	必ず気づいている				
	だいたい気づいている	ユーザ A (7) ユーザ B (7)	ユーザ E (5)		
	気づくときと気づかないときがある	ユーザ C (4) ユーザ D (4)		ユーザ F (3)	
	気づかない				

特に各設定の違いの効果を評価することとした. なお, 本実験の被験者については, グループ A は実験期間が短く (実際, グループ A の利用者がこの機能を利用できたのは 2 週間だけであり, 2 週間後も 8 人中全員はデフォルト設定である「通知画面の最前面ウインドウ表示, サウンド鳴動」で利用していた), この軽減策と通知機能設定の意味をよく理解している被験者が必要であったことから, 本評価実験ではグループ B の 8 人を被験者とし, うち 6 人から回答を得た.

モバイルアクセス通知機能をどのように設定しているかを質問した結果と, 他の設問で「他ユーザからモバイルアクセスがあった場合どの程度自分が気づいていると思うか」を質問した結果のクロス分析を行った結果を表 4 に示す. なお, 表 4 上にはさらに実際の回答者の分布を記し (A から F の 6 人), ユーザ名の下の括弧内の数値は, 当該ユーザが回答したプライバシ侵害感の点数 (映像, オンライン状態, メッセージの 3 項目の単純合計) である.

結果としては, グループ B の回答者 6 人のうち 4 人がデフォルト設定 (設定 A) のまま利用していたが, 表 4 を見ると, モバイルアクセス通知機能を強く (よく気づくように) 設定している人ほど (設定 A が最も強い), 「他ユーザのモバイルアクセスに自分は気づいている」と感じている. したがって, 期待した効果を実現したといえるが, ここで注目すべきこととして, そのような人 (自分は他人のモバイルアクセスの事実気づいていると思う人) ほどプライバシ侵害感 (括弧内の数字) が大きい傾向にあることが分かった.

一般社会においても周囲の動向を気にする人は自分が周囲からどう見られているかを気にする傾向があると思われるが, 本システムにおいても, 同様の傾向はあるようだ, しかし今回の実験結果の検定を試みたが

母数が少ないこともあり統計的な有意性を発見することはできなかった。

4.4 その他の評価結果（プライバシー侵害感の相対性に関する評価）

今回の評価実験に際し、筆者らはグループ B の被験者への質問表には、評価実験 2, 3 用の質問だけではなく、メディア空間利用初心者であるグループ A に質問するには適さないと思われる複雑な概念を含む）特段の仮説の設定に基づかない多く（合計 34 問）の質問を含めることとし、その中から注目すべき回答が見つかった場合にはその内容を評価することを企画した。その結果として出現したのが、表 5 に示す質問内容に対する回答であるので、その概要を紹介する。

各質問に対する回答は「強く感じる」、「少し感じる」、「あまり感じない」、「まったく感じない」の 4 つであり、これらにそれぞれ 4 点～1 点を与え、回答者全員（6 人）の平均得点を求めたが、その結果「他者の映像を閲覧することでその人のプライバシーを侵害していると感じる」との質問（3）の回答の点数が質問（1）に比べて有意に高かった（ $T(10)=1.98, P=0.037<0.05$ ）。

自分が「見られる」プライバシー侵害感問題に加えて、自分が「見る」ことで他者のプライバシーを侵害する感覚を気にするユーザがいることはこれまで筆者らもときどき気づいていたが、後者の方が点数として大きいことは予想できなかった。

4.5 「自分が他者に映像を閲覧されること」より、「自分が他者の映像を閲覧する」ことの方が心理的抵抗感がより大きいという問題について今回、表 5 の調査により現れた標記の問題は、これまでのメディア空間研究では触れられていない問題で

ある、「プライバシー侵害感の相対性（Relativity）」の問題の表層化である可能性が高い。

従来のメディア空間研究では、プライバシー侵害問題とは「自身の映像を閲覧されることに関するプライバシー侵害感（被監視感）、つまり「他者から自分の映像を閲覧されるようなシステムを使いたくない」という意識に関する問題であり、それを解消する技術に関する研究であった。しかし、もし「他者の映像が見えてしまうようなシステムを自分は使いたくない」という感覚がメディア空間システムのプライバシー侵害感の本質であるならば、その解決には別の技術が必要なはずである。その意味において、もし今回の評価結果がそれを発見しているのであれば、重要な問題である。また、これは映像に限らずプライバシー侵害全般に関連する問題である可能性も推測される。

4.6 前節のような問題を従来研究ではなぜ見過ごしてきたか

メディア空間の研究者、あるいは長期利用者は、PC に接続したビデオカメラが自分を向き、その映像が同僚に送信される状態に慣れきっている。特に研究者の場合には実装開発とテストを行う過程で自分のデスクの周辺に十数台の PC を並べ、それに接続されたビデオカメラがいっせいに自分の顔を向き、サーバに送信されているという状況がよくある（映像伝送の動作確認のために、動く被写体として自身のカメラ映像が最も使いやすいため。図 8 に例を示すような状態）。したがって、自身の勤務状況映像を常時撮像され、それが遠隔地のどこかに送られることに関して普通の人に比べて鈍感になってしまっている可能性がある。しかし一方で、他メンバからの映像は通常その受信・表示の動作状況をざっと確認する程度であり、じっくりと閲覧し行動を確認するわけではないので、それに関する抵抗感は普通の人間と同じレベルのままであると思われる。そのように推測すると、表 5 に示す結果と一致する。

表 5 グループ B に対するアンケート結果
Table 5 Results of questionnaire to group B.

質問内容	点数
(1) PC からアクセス中に他ユーザからモバイルアクセスがあり、あなたの勤務状況映像が閲覧される場合、あなたは自分のプライバシーが侵害されていると感じますか	1.833
(2) 携帯電話機でアクセスした際、あなたがアクセスした事実が PC 端末ユーザに通知されますが、それによりあなたは自分のプライバシーが侵害されていると感じますか	1.667
(3) 携帯電話機でアクセスし他ユーザの勤務状況映像を閲覧する際、あなたはその人（相手）のプライバシーを侵害していると感じますか	2.833



図 8 メディア空間システム開発中の画面例

Fig. 8 Building media space system using engineers' video.

表 6 メッセージ書き込み件数からみた本システムへの接続端末種別と、利用活性度推移

Table 6 Terminals used to access the system, and the user activity level, observed from the message count.

	グループ A (9名合計)						グループ B (8名合計)		
	第一期間			第二期間			1ヶ月	1日平均	比率
	1ヶ月	1日平均	比率	1週間	1日平均	比率			
PC 端末からの書き込み	135	4.50	100.0%	46	6.57	75.4%	221	7.37	75.7%
モバイルからの書き込み				15	2.14	24.6%	71	2.37	24.3%
合計 (件数)	135	4.50	100.0%	61	7.29	100.0%	292	9.73	100.0%

4.7 追加評価実験

4.5 節の発見後、その推測事項の真偽を探るため、グループ A (利用初心者グループ) に再度注目し、これを被験者として表 5 と同じ質問を行った ($n=8$)。結果として、質問 (1) への回答の平均点数は 2.625、質問 (2) も 2.625、質問 (3) への平均点数は 3.125 であった。また、人数で質問 (1) と質問 (3) への回答点数の大小を比べると、前者の点数が大きい者が 2 人、後者が大きい者が 5 人、同一点数が 1 人であった。これにより、グループ A にもグループ B と同様の傾向、すなわち「自分が他者の映像を閲覧する方がプライバシー侵害感が強い」傾向は観察されたが、有意な検定結果は得られなかった ($T(14)=-0.46, P=0.326$)。しかし、グループ A の被験者もこの評価の時点ですでに利用開始から約 10 カ月を経過してしまっており、必ずしも「メディア空間の利用初心者」とはいえなくなってしまっており、利用状況の観察からもグループ B と同様の慣れが発生している傾向が見られるので、やはりこの問題に関する今後の追加研究が必要であると考える。

4.8 評価実験期間中のコミュニケーション活性度推移

研究方針に示したように、本研究の目的が最終的に達成される状態とは (プライバシー問題だけではなく) PC 端末、携帯電話機のいずれから接続してもユーザがグループ意識やグループの一体感を感じられ、両端末相互間を含む全ユーザのコミュニケーションが活性化されることである。しかし、グループ一体感の直接的な測定は困難である。アクセス頻度の測定が手がかかりになると思われるが、評価実験期間中のグループ A および B の平日 (勤務日) のアクセス頻度は各ユーザともほぼ毎日 (かつ終日) であった。そこで、今回はグループ一体感と関連する指標であると思われ、またコミュニケーション活性化の直接的な把握指標となる、メッセージ書き込み件数に注目する。

メッセージ書き込み回数をデータベースより集計した結果を表 6 に示す (データベースからの集計であり、アンケート調査に回答しない者も含むため、人数は被験者とは異なる)。なお、特にモバイルアクセスは休日の利用も見られたため、1 カ月または 1 週間を 1 日平均に換算する際には休日の日数も加えた (PC 端末、モバイルとも)。グループ A の 2 つの期間を比較すると、モバイルアクセスが可能になった後は PC 端末からの書き込みも増加し、コミュニケーション件数が増えていることが分かる。なお、メンバ構成が違ってもかわらずグループ A の第 2 期間 (モバイルアクセスを全員が利用した後の期間) とグループ B との比較において、メッセージ書き込みに利用した端末 (PC or 携帯) の比率はほぼ同じという結果になった。なおグループ B の被験者へのアンケート調査では、モバイルアクセスを利用する場合の状況についても詳細に質問した。その結果は表には示していないが、就業時間中の外出・出張中と、帰宅後の自宅からの利用の 2 つが最も多いことが分かった。また通勤中、休日や平日帰社後の私用外出先からの利用をすると回答したのも比較的多くいた。出張中など業務理由の離席中だけでなく、就業時間外の利用が多いことは、本システムにモバイルアクセス機能を付加したことによりグループ意識や一体感がより高まった結果であると筆者らは直感的に感じているが、その定量的評価については今後の課題である。

5. 関連研究

メディア空間システムの著名な従来研究は前述したが、ここでは本研究に関連する周辺分野の従来研究、および本研究との相異について記す。

5.1 携帯電話機等を端末として用いるアウェアネス情報共有システム

携帯電話機等を用いたアウェアネス情報取得または共有システムの従来研究が以前より存在する。Sen-

Say⁹⁾ は、携帯電話機と接続できるセンサボックスに 3 次元加速度、照度、温度および音量（ノイズ）の各センサ、およびそれらから出力されるデータを処理する Decision Module を内蔵し、同 Module がユーザの置かれている状況を Uninterruptible, High Activity, Normal, Idle のいずれかと判定してその結果を携帯電話機に伝え、電話機の着信音量やパイプレータの利用を制御する。その結果 Context-Aware な携帯電話機が実現できたとしている。しかし取得したユーザの状況情報はそのユーザ自身の携帯電話機の制御にのみ用いており、その情報を他のユーザと共有することは行っていない。

野田らによる研究¹⁰⁾ では、携帯端末に加速度、照度、温度の各センサを実装し、屋外を移動する利用者の身体に装着させて移動させた結果、主に照度および温度センサからユーザが屋内にいるか屋外にいるかが推測でき、また加速度センサから歩行中かどうか（さらに、電車乗車中であるかどうかの可能性）を推測できたこと、およびそれらの情報を PHS 通信または無線 LAN 通信を経由してサーバに送信し、利用者間でそれらの情報を共有するシステムを構築できたことを報告している。しかしモバイルユーザの状況情報を共有できることを確認できたものの、協調作業や情報共有にその成果を適用するのは今後の課題であるとしている。

黒田らの研究¹¹⁾ によるアウェアネス情報共有システムは、42 インチの大型ディスプレイ、PC、PDA、携帯電話機のそれぞれをサーバを介して接続し各端末相互間での情報共有を可能にしたシステムであり、たとえば携帯電話機からサーバにアクセスして PC ユーザのアウェアネス情報を閲覧したり、PC ユーザや携帯電話機ユーザのアウェアネス情報を大型ディスプレイに表示したりすることができる。また共有できるアウェアネス情報はユーザの自己申告入力による現在位置等に加え、ユーザ端末が PC である場合、PC に接続した赤外線センサから取得した在席情報や PC で利用中のアプリケーション情報をサーバに送信し他のユーザと共有することも可能である。しかしこのシステムでは映像を扱うことはしておらず、また、プライバシー侵害問題に関しても研究対象としていない。

そのほかにも、携帯電話機等の中でアウェアネス情報の共有を行う研究として Awarenex¹²⁾ や The AWARE mobile phone¹³⁾ などがあるが、いずれも映像の送受信を行うことはできない。

すなわち、上記の各従来研究はアウェアネス技術を携帯電話機等を用いていかにユビキタス化された技術

に発展させるかにつき模索している段階にはあるが、本研究で扱うプライバシー侵害問題に関しては考慮していない。

5.2 共有スケジューラやアウェアネス情報共有システムにおけるプライバシー問題研究

映像を用いないスケジューラやアウェアネスシステムにおいてもプライバシー侵害問題は課題であり、それらを解決しようとする従来研究が存在する。アウェアネス情報を示す道具として従来から存在する「在室表」に注目し、それをメタファとして用いたシステムである Extended Destination Board¹⁴⁾ は、入力済の個人スケジュールと、ユーザの携帯電話機に表示される場所リストからユーザが手動選択して申告する位置情報をもとに、ユーザの状況・状態を推定しユーザ間で共有するシステムである。しかもそれらの情報をユーザ全員に公開することがプライバシー侵害につながる恐れがあることに着目し、解決策として各ユーザが閲覧許可者をデータベースに登録し、許可された他ユーザのみが当該ユーザの状態推定結果を閲覧できるようにしている。

また、高橋らは会議室予約情報、PC ステータス、RFID による所在地情報を複合的に用いてオフィスユーザのプレゼンス状況推定を行い、その結果を一覧表示するシステムを開発し¹⁵⁾、そのプレゼンス情報を公開することに関するユーザの受容性に関して調査している。それに際し、相互に了承したユーザ間のみでプレゼンス情報を公開する動作とした時期と、了承は行わずに全員に公開する動作とした時期があり、その違いを調査した結果、プライバシー公開について抵抗感を感じたとするユーザが前者では全ユーザの約 1 割、後者では 3 割であったという報告を行い、その結果として、この種のシステムでは公開範囲や公開方法に関してユーザが自ら選択可能とすることが必要であろうと結論づけている。

一方、平田らは従来の状況情報共有システムが「情報を知られたくない場合であっても相手に知られてしまうことがプライバシーの点で問題である」として、システムを利用していないユーザや自身の情報を開示しないユーザには自身の情報を伝送しないシステムを開発しその効果を確認したが¹⁶⁾、今後はユーザの状況情報を自動判定する必要があるだろうとしている。

以上 3 つの従来研究例のように、共有スケジューラやアウェアネス情報共有システムにおいてプライバシー侵害問題に着目した研究はあるが、いずれもユーザ自身がプライバシーを公開する相手やグループを選択し、それに対応した制御で解決しようとするにとど

まっている。また、映像を扱ったり携帯電話機等を用いたりすることに関連する研究は行われていない。

5.3 映像サーベイランス(監視カメラシステム)におけるプライバシー問題研究

監視カメラによる映像サーベイランスシステムは、通常その映像伝送が片方向であり、多地点間の映像共有によりネットワーク情報共有空間を創造しようとするメディア空間システムとは目的としても技術的にも違いが大きい。しかし近年、安全・安心な社会システム構築ニーズが全世界的に高まる中でその研究が活性化してきており、その中では「セキュリティとプライバシーのバランスをとる」ことに関する研究も行われている。PriSurv (Privacy Protected Video Surveillance System)¹⁷⁾ではプライバシーを保護しつつ監視することを目的に各種実験を行った結果、被写体となる被験者により撮像画像の開示に関する寛容度が異なることを確認し、そこで被写体と観察者(警察、警備員等)の関係によって細かい粒度で情報開示を制御する仕組みをとり入れ、また視覚的抽象化によるプライバシー保護機能の実現を目指している。しかしその研究過程において「プライバシーとは心理学的問題、かつそもそも個人が個人の領分と考える範囲に依存する概念であるため、個人性や主観性が強く、自身の容姿が映った映像を他者に見せる場合、どこまで開示すればプライバシーを侵されたと感じるかは個人によりまちまちであるため、これを工学的に扱うのは容易ではない⁷⁾」との見方を示し、工学的アプローチの限界を強調している。なお、携帯電話機等を監視用端末とした場合の研究は行っていない。

6. おわりに

PC 端末に加えて携帯電話機を端末として利用することができるメディア空間システムである「e-office Mobile Access」を開発した。そして、

- 全員利用可能ルール(同一 ID・パスワードルール)
- 被閲覧事実通知ルール

の実装を行うことにより、携帯電話機からメディア空間システムの内容を閲覧する場合に PC 端末ユーザのプライバシー侵害感を軽減できることを確認した。携帯電話機ユーザ側のプライバシー侵害感は、メディア空間へアクセスした事実を PC 端末ユーザに知られることについては少なかった。また、携帯電話機から接続する機能を加えることにより、PC 端末ユーザ、携帯電話機ユーザ両者のコミュニケーションを活性化することがメッセージ書き込み件数から見る限り分かり、したがってグループ体感を強化する効果もあるものと

推測される。

一方、実験前に予期しなかったこととして、携帯電話機ユーザが PC 端末ユーザの映像を閲覧する場合に、「閲覧する側が閲覧される側よりプライバシー侵害感が強い」という実験結果が得られた。

従来研究においては、メディア空間システムの問題点である Threat of Privacy Violation 問題とは「誰かが自分の知らない間に自分の映像を監視し、自分のプライバシーが侵害されているのではないか」という不安の問題であるとされていたが、本研究結果では、メディア空間システムのユーザは「自身の映像が閲覧されることにより自身のプライバシーが侵害される」こと以上に、「他者の映像を閲覧することによりその人のプライバシーを自身が侵害してしまう」ことの方をより強い心理的抵抗感として感じている。このメカニズムに関しては今後さらなる研究が必要であると考えられる。

参考文献

- 1) Angiolillo, J.S., Blanchard, H.E., Israelski, E.W. and Mane, A.: *Video-Mediated Communication*, pp.51-73, LEA Press, New Jersey (1997).
- 2) 岡田謙一：情報共有空間における協同、情報処理, Vol.48, No.2, pp.123-127 (2007).
- 3) Dourish, P. and Bly, S.: Portholes: Supporting Awareness in a Distributed Work Group, *Proc. ACM Conference on Human Factors in Computer Systems CHI'92*, pp.541-547, ACM Press (1992).
- 4) Lee, A. and Girsensohn, A.: Design, Experiences and User Preferences for a Web-based Awareness Tool, *International Journal of Human-Computer Studies, Special Issue on Awareness and WWW*, pp.75-107, Academic Press (2002).
- 5) 榊原 憲, 加藤政美, 田處善久, 宮崎貴識: メディア空間による分散勤務者のコミュニケーション支援システム「e-office」, 情報処理学会論文誌, Vol.43, No.8, pp.2821-2831 (2002).
- 6) 榊原 憲, 田處善久: メディア空間によるコミュニケーション支援システムの適用可能グループに関する研究, 情報処理学会シンポジウムシリーズ, Vol.2006, No.12, グループウェアとネットワークサービスワークショップ 2006 論文集, pp.91-96 (2006).
- 7) 馬場口登: プライバシーを考慮した映像サーベイランス, 情報処理, Vol.48, No.1, pp.30-36 (2007).
- 8) 榊原 憲: 米国企業による知的財産事業化の一事例研究, 経営情報学会 2007 年春季全国研究発表大会予稿集, pp.286-289 (2007).

- 9) Siewiorek, D., Smailagic, A., Furukawa, J., Krause, A., Moraveji, N., Reiger, K., Shaffer, J. and Wong, F.L.: SenSay: A context-aware mobile phone, *Proc. 7th IEEE International Symposium on Wearable Computers*, pp.248-249 (2003).
- 10) 野田敬寛, 吉野 孝, 宗森 純: センサ情報を共有可能なモバイルシステムの開発と適用, 情報処理学会研究報告, マルチメディア通信と分散処理研究会, DPS-116-10, pp.55-60 (2004).
- 11) 黒田淳平, 吉野 孝, 宗森 純: 多種の情報機器を利用可能なアウェアネス情報共有システム, 情報処理学会研究報告, 2003-GN-47, pp.1-6 (2003).
- 12) Tang, J.C., Yankelovich, N., Begole, J., Kleek, M.V., Li, F. and Bhalodia, J.: ConnNexus to awarenex: extending awareness to mobile users, *Proc. SIGCHI Conference on Human Factors in Computing Systems*, pp.221-228 (2001).
- 13) Bardram, J.E. and Hansen, T.R.: The AWARE architecture: supporting context-mediated social awareness in mobile cooperation, *Proc. CSCW2003*, pp.192-201, ACM Press (2003).
- 14) Tsuchimochi, Y., Takahashi, S. and Tanaka, J.: Extended Destination Board: Supporting Awareness for Cooperation working and Informal communications, *Proc. KICSS2006, The 1st International Conference on Knowledge, Information and Creativity Support Systems*, pp.59-65 (2006).
- 15) 高橋一成, 桑田喜隆: プレゼンスサービスを活用したオフィスのコラボレーション支援, 情報処理学会論文誌, Vol.48, No.1, pp.2-15 (2007).
- 16) 平田俊之, 国藤 進: プライバシー保護を可能とする状況情報共有システムの開発と運用実験, 情報処理学会論文誌, Vol.48, No.1, pp.189-199 (2007).
- 17) Koshimizu, T., Toriyama, T. and Babaguchi, N.: Factors on the Sense of Privacy in Video Surveillance, *Proc. CARPE'06, The 3rd ACM Workshop on Continuous Archival and Retrieval of Personal Experiences*, pp.35-44,

ACM Press (2006).

(平成 19 年 4 月 9 日受付)

(平成 19 年 7 月 3 日採録)



榊原 憲 (正会員)

1984年東京工業大学工学部経営工学科卒業。同年キヤノン(株)に入社。現在キヤノン電子(株)キヤノン電子情報セキュリティ研究所所属。東京工業大学大学院イノベーションマネジメント研究科博士後期課程在学中。2001年度本会全国大会グループウェアとネットワークサービス特別トラック優秀発表賞, 2002年度本会論文賞, 2003年度本会山下記念研究賞, GNWS2006 ベストプレゼンテーション賞各受賞。日本テレワーク学会理事。電子情報通信学会, 日本経営工学会, 経営情報学会, 日本 MOT 学会各会員。



比嘉 邦彦

東京工業大学大学院イノベーションマネジメント研究科教授。同研究科技術経営専攻長。1988年米国アリゾナ大学経営情報システム専攻にて Ph.D. を修得。以来, 同大学講師, ジョージア工科大学助教授, 香港科学技術大学助教授を経て 1996年東京工業大学経営工学専攻助教授。1999年より現職。分散環境におけるコミュニケーションと情報共有支援システム, E-コマースの評価・分析モデル, 組織戦略としてのテレワーク, 持続可能な地域社会モデル等について研究。高知県アウトソーシング検討委員会委員長, テレワーク推進フォーラム副会長・普及部会部長, 社団法人日本テレワーク協会アドバイザー。日本テレワーク学会前代表。ACM, AIS, INFORMS, 経営情報学会等各会員。