PC環境ローミング技術を用いた安心なテレワーク支援システム

飯塚重善[†] 小川克彦[†] 中嶌信弥[†,☆]

昨今，自宅等事業所から離れた場所から通信回線を通して作業を行う，いわゆる「テレワーク」に対する試みが，各企業等において様々なスタイルでなされてきている．特に，モバイル型テレワークについては，移動中にも効率良く仕事を行うことができる反面，ノートPC等の情報機器を持ち運んで利用するため，情報機器のセキュリティ管理も必要になる．筆者らは，モバイル型テレワークにおける，仕事の場に関するフレキシビリティを活かし，かつ，情報機器における情報セキュリティの課題を払拭することで，安全で快適なテレワークを実現するために，ノートPC等の情報機器は持ち歩かず，ICカードを持ち歩くだけで，モバイルオフィス等に設置されている共同利用パソコンを，まるで自分のパソコンを持ち歩いているような感覚で利用できる，PC環境ローミング技術を用いたテレワーク支援システムを開発した．そして，その評価のため，実際のビジネスパーソン146名に，本システムを用いたテレワークを実践してもらう実験を3カ月間行った．その結果，本システムの有効性および安心感について高い評価を受けた．また，システムの環境面での安心感の調査を行い，場所によるシステム利用時の安心度に差が生じることを明らかにした．本稿では，本システムのシステム構成，処理内容および評価実験の結果とそれに基づく考察を述べる．

Reassuring Telework Support System with PC Environment Roaming Technology

Shigeyoshi Iizuka,[†] Katsuhiko Ogawa[†] and Shinya Nakajima[†,☆]

These days, the trial to the so-called “telework” which works from the place distant from places of business, such as a house through a communication line has been made in various styles in each company etc. We developed the reassuring telework support system with PC environment roaming. Furthermore, in order to investigate the effect of this system, we conducted the trial by actual business person practice. The result shows our system was well accepted. This paper presents our system architecture and the trial.

1. はじめに

昨今，自宅等事業所から離れた場所から通信回線を通して作業を行う，いわゆる「テレワーク」に対する試みが，各企業等において様々なスタイルでなされてきている[1)~5)]．このテレワークは，経営者側の立場からは仕事の生産性向上やオフィスコスト削減，就業者の立場からは働き方のフレキシビリティを実現できるという点でその効果を期待されている．テレワークの形態を実施する場所で分類すると，自宅の書斎等で仕事を行う自宅利用型テレワーク，ある程度の情報通信機器やデスク，接客空間や秘書機能等を備えているサテライトオフィスを利用する施設利用型テレワーク，ノートPCやPDA等を活用して，移動中にも効率良く仕事を行うモバイル型テレワークがある[1),6)]．

テレワークについて頻繁に指摘される懸念は，テレワークで働く労働者がいだく孤立と孤独感であり，人間同士のコミュニケーション（情報伝達）の確保もきわめて大切である[2)]．こうした懸念を払拭する目的で開発されたものとして，すでに，遠隔地間をブロードバンドネットワークで結び，音声や映像通信を実現することにより，在宅勤務者のコミュニケーションを支援するテレワーク支援システム[7)]やつながり感に着目したテレワーク支援システム[8)]が実現されている．

特に，モバイル型テレワークは，情報通信の活用によって，利用者とその相手との距離が縮まり，移動中でも仕事が可能，等具体的なメリットが認識されやすい．つまり，無駄なモビリティを省き，必要なときに必要な場所で仕事を行い，ひいてはオフィスコストの削減にもつながるという合理性が受け入れられている．また，他の形態のテレワークと違い，運用方法によっては人事制度や評価等のマネジメントの仕組みを本質

† NTTサイバーソリューション研究所
NTT Cyber Solutions Laboratories
☆ 現在，エヌ・ティ・ティ アイティ株式会社
Presently with NTT-IT CO., LTD.

的に変えなくても導入可能であることから，営業部門等社外での活動の比率が高いオフィスワーカを対象として導入事例が増えている[6]．

しかしながら，テレワークを推進するうえでは，「仕事と仕事以外の時間の切り分け，公私の区分の明確化」や「テレワークに適した住宅整備や街づくり」といった自己管理や環境面の課題とともに，「情報セキュリティの確保」も重要な課題としてあげられている[1]．

システムに対する情報セキュリティは，サーバ，クライアント，ネットワーク等のシステム面を対象として，すでに企業内ネットワークへのアクセス制御やデータ保護の暗号化等の技術が実際に活用されてきている．ただし，モバイル型テレワークについては，ノート PC 等の情報機器を持ち運んで利用するため，情報機器のセキュリティ管理も必要になる．たとえば，コンピュータはそれ自体に資産価値があるため，盗まれる可能性がある．また，コンピュータだけでなく，情報を記録した媒体の保全や盗難防止策も立てておく必要がある．最近はスマートカード等小型大容量の媒体が普及しているため，情報を盗むのはますます容易になっている．また，ハードディスク等の固定媒体も盗難に遭う可能性は CD-R 等と同様と考えなければならない[9]．実際には，さらに，システムを利用する場所（環境）の安全性，すわなちシステム利用時の環境面のセキュリティにも注意する必要がある．特に，モバイル型テレワークのように，様々な場所を仕事の場とする際，その場所によって，システム利用時の安心感が異なってくることが予想される．

そこで筆者らは，まず，システム面のセキュリティ対策として，モバイル型テレワークにおける，仕事の場に関するフレキシビリティを活かし，かつ，上記のような情報機器に関する情報セキュリティの課題を払拭することで，安全で快適なテレワークを実現する方法について検討した．そして，ノート PC 等の情報機器は持ち歩かず，IC カードを持ち歩くだけで，モバイルオフィス等に設置されている共同利用パソコンを，まるで自分のパソコンを持ち歩いているような感覚で利用できる，PC 環境ローミング技術[10),11)] によるテレワーク支援システムを開発することとした．具体的には，この PC 環境ローミング技術により，情報機器を持ち歩かずに，モバイルオフィス等に設置されている共同利用パソコンを利用することで，テレワーク機器のセキュリティ管理の問題を回避することができる．さらに，共同利用パソコン上に個人の PC 環境を再現しており，これにより自分のパソコンを持ち歩いているのと同等の利便性を実現している．そして，利用終了後には，共同利用パソコン上に再現された個人の PC 環境の自動消去も実現しており，情報の漏洩の防止にも対応している．

ところで，ある PC 環境を別のパソコン上に再現する既存技術には，一般のアプリケーションを実行する方式で分けると，「サーバ実行型」と「クライアント実行型」とがある．まず，「サーバ実行型」は，アプリケーションをサーバ上で実行する形態をとっており，ユーザはそのサーバ配下のクライアントであれば，どこからでもサーバ上のアプリケーションを利用することができる，というものである．この例としては，VNC（Virtual Network Computing）[12)] や，「MetaFrame」（Citrix 社）[14)]，「Sun Ray」（サン・マイクロシステムズ社）[15)] といったサーバベースコンピューティング[13)] がある．これらは，クライアントからのマウス，キーボードの操作情報を受け取ったサーバが，デスクトップ画面更新情報をクライアントに返すことで実現しているため，クライアント PC のスペックは低くてよい反面，サーバや伝送路の負荷が大きく，“マルチメディアアプリケーションの動作が困難”，“スクロールが遅い” という欠点がある．特に，今回対象としているテレワークについては，不特定多数のユーザが同時に利用することが考えられる共同利用パソコンの状況においては，サーバ実行型では，クライアントの同時利用の台数の増加にともなうサーバ・ネットワークの負荷の増大により動作に影響が出やすい．一方，「クライアント実行型」はアプリケーションをクライアント上で実行する形態をとっている．この例としては，異なる OS のアプリケーションを実行する仮想計算機 vmware[16)] や，仮想計算機を介して実行イメージ（スナップショット）が異なるコンピュータ間を渡り歩く「ネットワークを渡り歩けるコンピュータ」[17),18)] があるが，これらは仮想計算機そのものであったり，仮想計算機ソフトを前提としたつくりをしており，いずれも処理速度面でつねにオーバヘッドを要求してしまう．筆者らが開発した PC 環境ローミング技術はクライアント実行型に位置づけられるが，利用中動作への影響を少なくするために，仮想計算機ソフトを利用せずに PC 環境の移行を実現しているため，処理速度面の問題も発生しない．また，ネットワークの負荷もクライアント利用開始時のみで伝送路への負荷は小さい．

筆者らはこれまで，PC 環境ローミング技術について，レンタルオフィスの共同利用パソコンへ適用することでその有効性を確認する実験を行ってきており[19)]，共同利用パソコンにおける PC 環境ローミングサービスとしては多くのモニタに受け入れられた，という結

果を得ている．だが，実際のテレワークシステムとしての有効性を確認するためには，システム面のセキュリティ対策の有無だけでなく，実際のテレワークに利用される様々なワークプレースにおいて，ユーザがシステムに対して安心だと感じていることを確認する必要がある．

そこで本稿では，筆者らが開発した，PC 環境ローミング技術を用いたテレワーク支援システムについて，実際のテレワークで利用される様々なワークプレースでの実証実験を行い，システムに対してユーザが感じる安心感を調査した結果について述べる．具体的には，上述のレンタルオフィスでの PC 環境ローミング技術の実験[19] よりも拠点数およびモニタ数を増やすことで実験の規模を拡大し，さらに実際のテレワークに利用してもらい，ユーザの安心感を調べることにより，本システムの，テレワークシステムとしての有効性の評価を行った．加えて，作業環境面の安心感については，実験に利用した拠点ごとに，モニタから安心感についてのアンケートを行い，ワークプレースによるユーザの安心感の差異を調査した．

以下，2 章では PC 環境ローミング技術の概要を，次に 3 章ではシステム構成および処理内容を，続いて 4 章では評価実験の内容，結果，それに対する考察，およびワークプレースの安心感についての調査結果を，そして，5 章にて結論としてまとめと今後の課題について述べる．

2. PC 環境ローミング技術

本章では，筆者らが開発した PC 環境ローミング技術の特徴と，実現のための方式について述べる．

2.1 実現内容

まず，PC 環境ローミング技術とは，以下の 2 つを実現する技術である．

(1) 共同利用パソコンに，自分用に設定した PC 環境を再現

IC カードを挿入するだけで，インストールしたアプリケーションのファイルを含むユーザの PC 環境を，サーバにバックアップ・リストアすることで，そのユーザが設定した PC 環境を共同利用パソコン上に再現することができる．

(2) 高セキュリティで安全な PC 利用を実現

パソコン利用終了時には，使用痕跡を自動的に消去する．よって，ユーザのデータや設定環境情報がパソコン上に残らず，次の利用者に個人のデータや情報が漏れることはない．さらに，IC カード内の鍵でユーザのデータ内容や設定環境情報を暗号化してサーバに保存する．したがって，サーバ管理者さえもその内容を参照することができない仕組みになっている．

3. システムの概要

本章では，前章で述べた PC 環境ローミング技術を用いて筆者らが構築したテレワーク支援システムについて，システムの全体構成，処理概要，モジュール構成，および利用手順を述べる．

3.1 システムの全体構成

本システムは，サーバに，IP ネットワーク（インターネット）を介して接続された複数台のクライアントから構成される（**図 1**）．クライアントは，公共施設等のモバイルオフィスの共同利用パソコンスペースに設置されることになる．サーバは，ユーザの PC 環境データを保管する装置であり，IP ネットワーク（インターネット）上に配置される．ここで，サーバはグローバルインターネット上のどこでも設置可であるが，ある会社の社内ネットワークのような，外部からのドメインアクセス自体に認証を要するドメイン内にサーバを設置する場合にはクライアントも同一ドメイン内に設置する必要がある．ユーザは，ロケーション A からロケーション B の間を IC カードのみを持ち歩くだけで，本システムを利用することができる．

3.2 処理概要

図 2 に，本システムの処理概略を示す．以下，各処理について詳細を述べる．なお，本システムでは，次項以降に示すそれぞれの処理を一連の処理として組み合わせ，新たなシステムを構成している．特に，本システムのポイントとなる，クライアントの 2 アカウント構成や，差分バックアップ機能については，それぞれ 3.2.2 項，3.2.3 項でその詳細を説明する．また，本システムでは，クライアントにおけるバックアップ処

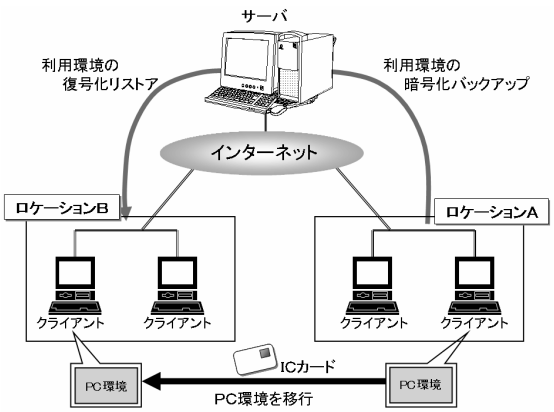

図 1 システムの全体構成
Fig. 1 System architecture.

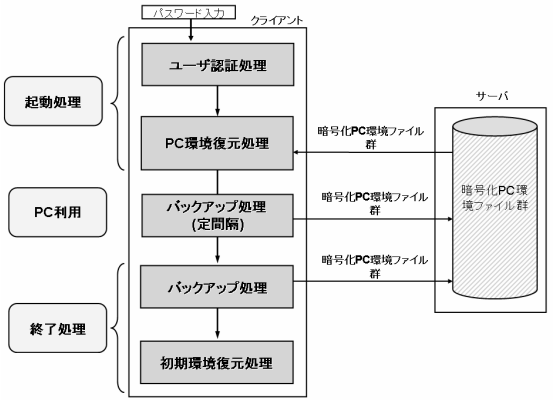

図 2 概略フロー
Fig. 2 Outline of processing.

理で，ユーザのデータ内容や設定環境情報を暗号化してサーバに保存している．ここで使用している暗号化処理は，秘密鍵暗号方式と公開鍵暗号方式を組み合わせた方式をとっている．データ本体の暗号化は秘密鍵暗号化方式（FEAL32x）で，共通鍵 Xi（鍵長 16 バイト）を使って行う．Xi 鍵は暗号化するとき，ランダムに生成されるものを用いる．データの暗号化完了後，Xi 鍵データを公開鍵暗号化方式で暗号し，Xi 鍵で暗号化されたデータと一緒にサーバに保存している．

3.2.1 ユーザ認証処理

IC カードは，ユーザ認証のトークンとして有効である．本システムでは，暗号鍵を IC カードに格納し，IC カードの PIN（カードパスワード）で開錠する方式とすることで，ユーザ認証が成功した場合においてだけ暗号鍵を利用でき，そのユーザの PC 環境データをその鍵で自動的に復号化するようにしている．

3.2.2 PC 環境復元処理

Windows 上に，あるユーザの PC 環境を構築するためには，そのユーザのアカウントで Windows を起動する前に，あらかじめそのユーザの PC 環境に関する情報を持っておく必要がある．そこで，本システムでは，クライアント内の OS 上に，“システム用アカウント” と，“ユーザ用アカウント” の 2 つの Windows アカウントを設け，プログラム内部でこの 2 つのアカウントを切り替えることで，ユーザの PC 環境復元処理を実現している．具体的には，利用開始時は，“システム用アカウント” でのログイン状態となっており，ユーザ認証処理後に，ユーザの PC 環境情報のダウンロード・データの復号化に続けて，ユーザアカウントの Windows へのマージを行う．この後，“ユーザ用アカウント” に切り替えて Windows を起動し直すことでそのユーザの PC 環境での立ち上げを実現している（**図 3**）．

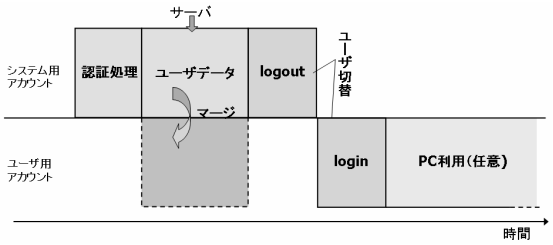

図 3 クライアント起動フロー
Fig. 3 Opening flow of client.

3.2.3 バックアップ処理

自分が設定した PC 環境を完全に復元するためには，自分が設定した情報を取得する必要がある．通常，ユーザが設定した PC 環境情報はパソコンのハードディスク内に保存されている．単純に考えれば，あるユーザが使っていたハードディスクの情報をすべてサーバ上にアップロードし，利用前にそのハードディスクの情報をダウンロードすることで実現できる．しかし，利用終了（利用開始）時に，ユーザが設定した PC 環境情報を含むハードディスクを丸ごとバックアップ（リストア）するのは，かなりの時間を要することが容易に想像できる．その結果として，ユーザをその分，待たせることになってしまう．そこで，本システムにおけるバックアップ処理では，「共通初期環境の導入」および「定間隔差分バックアップ方式」の 2 つの方式を実現することで利用終了（利用開始）時にバックアップするデータ量を削減し，その結果として利用終了（開始）時のユーザの待ち時間を短縮している．以下，この 2 つの方式の詳細を述べる．

(1) 共通初期環境の導入

本システムでは，起動されたクライアントのハードディスク内のデータは，**図 4** 中にあるように，「共通初期環境」と「ユーザの PC 環境」とに分けられている．「共通初期環境」とは Windows そのものや全ユーザに共通に提供されるアプリケーション等を含む環境で，ユーザが本システムを初めて利用する際に起動されたクライアントは，この「共通初期環境」のみで起動された状態となる．なお，実際の利用にあたって，ユーザは，この共通初期環境に対して，必要に応じてアプリケーションを追加したり，設定の変更を施したりしていくことで，本システム上に「自分の PC 環境」を構築していくことになる．

一方，「ユーザの PC 環境」とは，本システム利用中にユーザが施した設定変更情報や作成したファイル等，「共通初期環境」との差分にあたる．本システムに

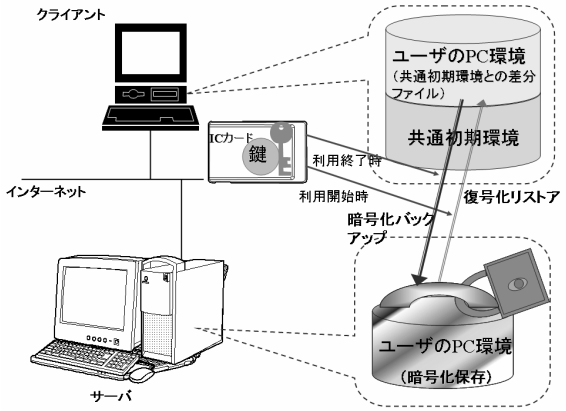

図 4 バックアップ処理
Fig. 4 Backup processing.

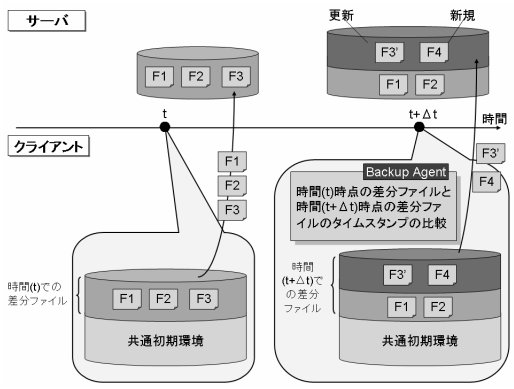

図 5 定間隔差分バックアップ処理の詳細
Fig. 5 Detail of difference files backup processing.

おけるバックアップ処理は，「ユーザの PC 環境」のみを対象としている（図 4）．こうすることで，サーバ〜クライアント間で行うバックアップ・リストアのデータ量を削減し，利用開始時・終了時の処理時間を短縮している．

(2) 定間隔差分バックアップ方式

終了時のバックアップデータ量をさらに削減するため，利用中のクライアントのハードディスクの状態を一定の時間間隔（Δt）でチェックし，共通初期環境との差分の発生を検出した場合は，そのつど，その時点で検出した差分のみを暗号化してサーバにバックアップする「定間隔バックアップ方式」を採用している．ただし，パソコン利用中は Windows によってロックされている常駐ファイル等もあるため，それらについては，終了プロセス起動後に自動的に暗号化されてサーバ上にバックアップされる．この定間隔差分バックアップ処理の詳細を，**図 5** の例を用いて説明する．

まず，ユーザの PC 利用において，差分ファイル F1, F2 および F3 が作成され，時間 t のタイミングでそれらの差分が検出されたとすると，その時点で，F1, F2 および F3 は自動的に暗号化されてサーバにバックアップされる．そして，その後の PC 利用において，F3 が更新され F3' となり，また新たに F4 が作成されたとすると，次のチェックタイミング t＋Δt で，それらの差分ファイルのタイムスタンプの比較が行われる．その結果として，F3 のタイムスタンプが更新されている F3'，および新規の F4 だけが自動的に暗号化されてサーバにバックアップされる（F1 と F2 はもうバックアップされない）．この方法で定間隔差分バックアップを実現している．

なお，この定間隔差分バックアップ処理のために，クライアントでのアプリケーション利用中，クライアントのメモリ上に定間隔差分バックアップ処理用のエージェント（プログラム）が常駐することになるが，十数 MB の消費容量で，クライアント（アプリケーション）の動作にはほとんど影響がない．

3.2.4 初期環境復元処理

初期環境復元処理とは，ユーザが利用したクライアントの作業領域を消去し，かつ，あらかじめ格納されている利用前の状態（共通初期環境）を自動的に復元する処理である．本システムでは，これらを一連の処理として自動的に行うことで，そのユーザに関する情報を次のユーザに見られないようにしている．具体的には，クライアントを初期状態に戻すために，市販のドライブシールド[20] を組み込み，これを実行する処理を，クライアントの終了処理の中に組み込むことで，作業領域の消去と初期環境の復元を自動的に行っている．このドライブシールドは，ファイルの新規作成や変更，削除等の操作をはじめ，パーティションのフォーマットや削除，レジストリやシステムフォルダへの変更操作を行っても，コンピュータを再起動するだけでそれらの操作は無効になり元の状態に戻る，という機能を備えている．クライアントの初期状態をドライブシールドで保護して，ユーザが本システムの利用終了時に，クライアントの利用終了プロセスを起動するだけで，ユーザの PC 利用によるクライアントのハードディスク内の変更等がすべて無効になり，初期状態に戻る．

3.3 モジュール構成

まず，前節までで述べた処理を実現するモジュール構成を**図 6** に示す．

サーバは LinuxOS をベースとして，クライアントとの通信を制御する「HTTP サーバ」およびクライアントとの間でユーザのデータや利用環境情報ファイル

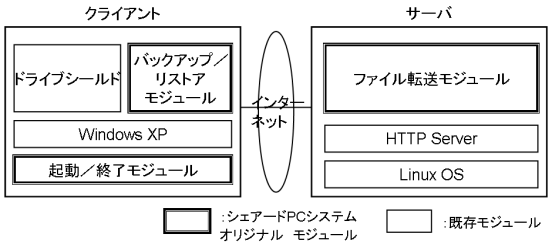

図 6 モジュール構成
Fig. 6 Diagram of module.

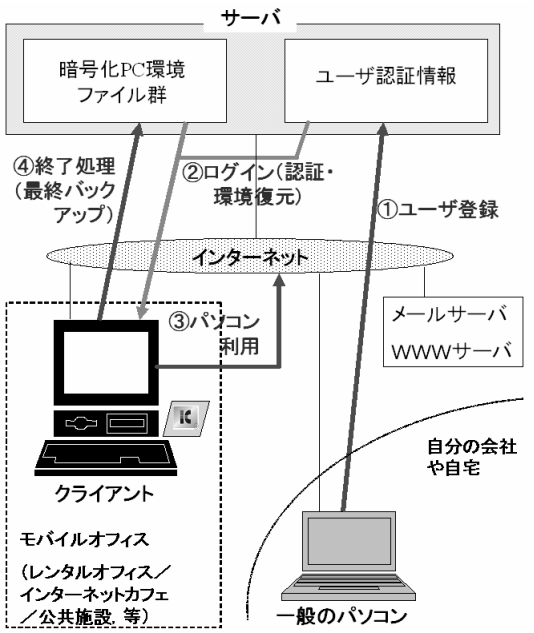

図 7 利用手順
Fig. 7 Procedure.

の受け渡しを行う「ファイル転送モジュール」とから構成される．一方，クライアントは WindowsXP をベースとして，ユーザのデータや設定環境ファイルをサーバとの間でバックアップ/リストアする「バックアップ/リストアモジュール」，ユーザの利用終了後に自動的に使用痕跡を消去し，クライアントの共通初期環境を復元させる「ドライブシールド」，およびクライアントの起動/終了を制御する「起動/終了モジュール」とから構成される．

3.4 利 用 手 順

本システムの利用手順を**図 7** に示す．

利用手順は，図 7 中の①→②→③→④→⑤の順となる．ただし，①は最初に 1 回行えばよい．以下，各手順について説明する．

① **ユーザ登録**

ユーザは本システムを使用するにあたり，前もって会社や自宅の一般のパソコンから本システムのサーバのユーザ登録用 URL にアクセスして，サーバに名前，連絡先 E メールアドレス等の利用者情報とともに，ユーザ認証情報（ユーザ ID，パスワード等）を登録しておく．このユーザ登録後に，システム（サーバ）管理者により，そのユーザ固有の秘密鍵の生成，書き込みやその秘密鍵を読み出すためのアクセスパスワードとしてユーザがユーザ登録時に入力したパスワードが設定された IC カードを，郵送やクライアント利用拠点等で受け取る．

② **ログイン（認証・環境復元）**

ユーザが，本システム利用のためモバイルオフィスに赴き，自分の IC カードをクライアントの IC カード R/W に挿入，パスワードを入力してログインすると，ユーザの正当性を認証するとともに，初めての利用の場合は共通初期環境が起動される（3.2.2 項で述べたように，ユーザは，この共通初期環境に，個々に必要に応じてアプリケーションのインストールや環境の設定変更を施していくことで，自分の PC 環境を構築していく）．2 回目以降の利用においては，前回利用の③および④（後述）のステップで保存された PC 環境がサーバから暗号化 PC 環境ファイル群としてダウンロードされ，クライアントで自動的に復号化され，PC 環境の復元が行われる．

③ **パソコン利用**

②でユーザの PC 環境が復元されたクライアントを実際に利用する．なお，このステップにおいて，クライアントでは，3.2.3 項で述べた定間隔バックアップ処理が自動的に行われている．

④ **終了処理（最終バックアップ）**

ユーザは，作業終了に際して，利用終了プロセスを起動する．すると，③のステップで，Windows によってロックされていたためにバックアップできなかった常駐ファイル等が自動的に暗号化されサーバ上にバックアップされる（最終バックアップ）．この最終バックアップが終わると，3.2.4 項で述べたように，自動的にドライブシールドが起動される．続いて，クライアントは自動的に再起動され，共通初期環境で立ち上げる．これによって，ユーザの使用痕跡は自動的に消去され，セキュリティを確保することができる．

上記のような処理で，ユーザは，自分の IC カード

を挿入し，パスワードを入力するだけで，共同利用パソコン上に，自分用に設定したPC環境が自動的に再現され，利用後も，クライアントの利用終了プロセスを起動するだけで，データのバックアップおよび消去は自動的に行われ，かつセキュリティが確保される．

4. 実　　験

本システムを，実際のテレワークに利用してもらい，ユーザのシステムに対する安心感を調べることにより，本システムの，テレワークシステムとしての有効性の評価を行った．加えて，作業環境面の安心感については，実験に利用した拠点ごとに，モニタに対して安心感についてのアンケートを行い，ワークプレースによるユーザの安心感の差異を調査した．以下，その実験の概要，結果および評価，そして調査の結果について示す．

4.1 概　　要

本実験では，グローバルインターネット上にサーバを設置し，**表1**に示す10カ所のワークプレースをモバイルオフィスとして，それぞれの場所にクライアントを1〜3台ずつ（計14台）設置して，テレワークへの適用実証実験を3カ月間実施した．146名のモニタが，業務のホームベースはモニタ自身の会社のオフィスに置き，必要に応じてワークプレースを利用して直行直帰するという形態で本システムを利用することでテレワークを実施した．また，利用終了後に，アンケートによる調査を実施することで本システムの有効性の主観評価を行った．今回の実験で使用したクライアント端末およびサーバ機のスペックを**表2**に示す．

表1 ワークプレース一覧
Table 1 Work-place list.

ワークプレース	端末台数
レンタルオフィス A	3
ホテル内ビジネスセンタ	1
カフェA	1
カフェB	2
ビジネスクラブ	1
駅	1
空港1ラウンジ A	1
空港1ラウンジ B	1
空港2ラウンジ A	1
空港2ラウンジ B	1

4.2 結果および考察

4.2.1 システムに対する安心感

アンケートでは，モニタに対してシステムの利用に関する以下の質問3つに答えてもらった．

- 今後もこのシステムを使いたいと思った．
- PCの使用痕跡を消去してくれるのが安心だった．
- このシステムのセキュリティは十分だと感じた．

すべての質問については，**図8**に示す5段階評価による回答を求めた．調査は実験終了後に質問紙を配布することで行った．すべての質問に対する回答があったものを有効回答とし，77の有効回答を得た．アンケートの集計結果を**図9**に示す．

まず，質問1の結果から，本システムを今後も使いたいと思ったモニタが82%に達しており，システム全般の評価は非常に高いといえる．また，質問2の結果から，本システムのPC使用痕跡消去機能に対しても，73%のモニタが安心だと感じ，高い評価が得られたといえる．実際に，実験中や実験終了後に，「前に使っていた人の情報や設定が残っていた」という報告も受けておらず，複数のモニタにヒヤリングをかけてもそのような事象の発生はなかったようである．さらに，質問3の結果を見ると，本システム全体のセキュリティについても，72%のモニタが十分であると感じており，本システムが，安心なテレワーク支援システムとして十分な品質にあるという結果が得られた．

ここで，質問3において「十分である」と感じるこ

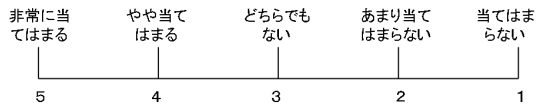

図8 アンケートにおける評価スケール
Fig. 8 Evaluation scale.

表2 実験環境の詳細
Table 2 Detail of environment for experiment.

各部		スペック
クライアント	CPU	Pentium4 2.66 GHz
メモリ		1024 MB
HDD		160 GB
OS		WindowsXP SP1
アプリケーション環境		MS OfficeXP professional, Norton Anti Virus2003
その他		IC カード R/W
サーバ	CPU	Pentium 4 2.66 GHz
メモリ		1024 MB
OS		TurboLinux8 server edition

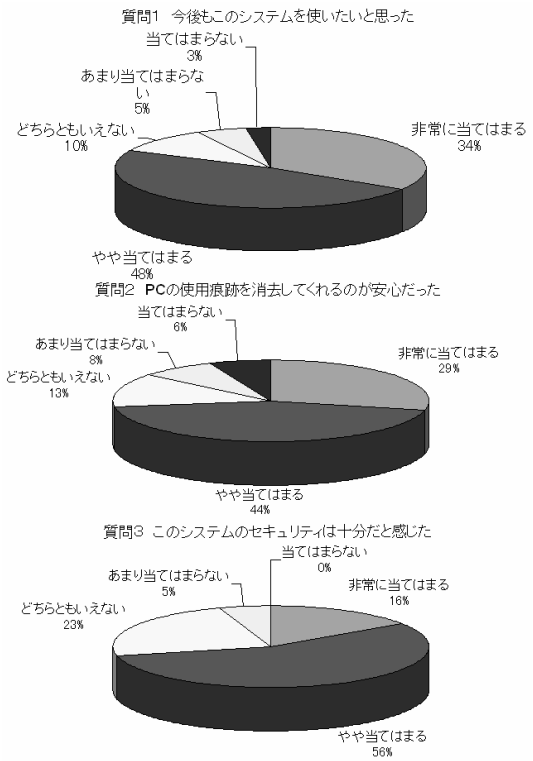

図 9 アンケート結果
Fig. 9 Enquete result.

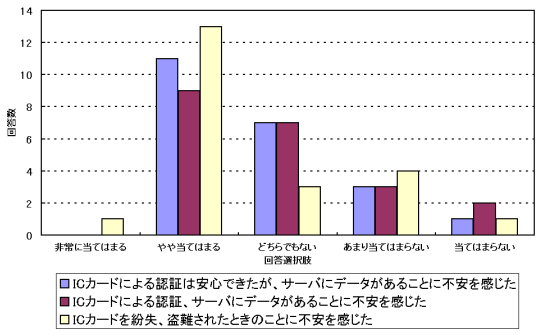

図 10 本システムへの不安
Fig. 10 Fear to our system.

とができなかった 28%（22 名）のモニタに対して，さらに，本システムへの不安に関する質問を行った．ここでも図 8 に示す 5 段階評価による回答を求めた．すべての質問に対する回答があったものを有効回答とし，21 の有効回答を得た．集計結果を**図 10** に示す．

この結果から，依然として，IC カードによる認証，IC カードの紛失，盗難への不安，サーバにデータがあることへの不安があることが分かった．よって，認証については，不変な身体的特徴を利用した認証（バイオメトリクス）等，持ち歩きの必要がない方法を採用する方向での検討が必要と考えられる．

4.2.2 利用環境に対する安心感

次に，システム利用時の環境面でのセキュリティに関して，同じシステムを利用する場合の，場所による安心度の差を調査した．ここでは，ユーザがワークプレースでシステムを実際に利用する際に安心と感じる度合いを，そのワークプレースにおけるシステムの安心度としてワークプレースの安心度の評価を行った．調査の方法は，前節と同じ実験モニタ 77 名に，各ワークプレースにおける本システム利用時に安心の度合いについて答えてもらうことで行った．ここでも，図 8 に示す 5 段階評価による回答を求めた．なお，調査の対象としたワークプレースは，5 名以上のモニタが利用したワークプレース 6 カ所に絞った．

まず，各ワークプレースでの安心感についての集計結果を**図 11** に示す．この結果から，レンタルオフィス A，ビジネスクラブおよび空港 1 ラウンジ A の 3 つの評価が良かった．特に，レンタルオフィス A およびビジネスクラブについては否定的な回答も見られなかった．一方，この 3 カ所以外の場所についてはけっして安心度は高くない．システムだけでみた場合のセキュリティの評価は，4.2.1 項で示したように高いにもかかわらず，利用する場所によって安心度に明らかな差が出ることが確認できた．この差は，レンタルオフィスおよびビジネスクラブがそもそもビジネスパーソン向けに構築された環境であることに起因していると考えられる．すなわち，安心してシステムを利用するためには，システムを使用する環境面についても配慮が必要であるといえる．

5. 結　　論

IC カードを持ち歩くだけで，モバイルオフィス等に設置されている共同利用パソコンを，まるで自分のパソコンを持ち歩いているような感覚で利用できる，PC 環境ローミング技術を用いたテレワーク支援システムを開発した．そして，実際のビジネスパーソンの業務に利用してもらい，システムに対する安心感についてのアンケート調査を行うことにより，安心なテレワーク支援システムとしての有効性を評価する実験を実施した．その結果，本システムについて高い評価を得，また，セキュリティについても十分であるとの評価を得た．ただし，IC カードの利用やデータがサーバにあることについて一部不安を感じているモニタがおり，今後は，バイオメトリクス認証等，盗難，紛失の恐れのない認証手段を利用することも視野に入れて検討していく必要があることが分かった．しかし，バイ

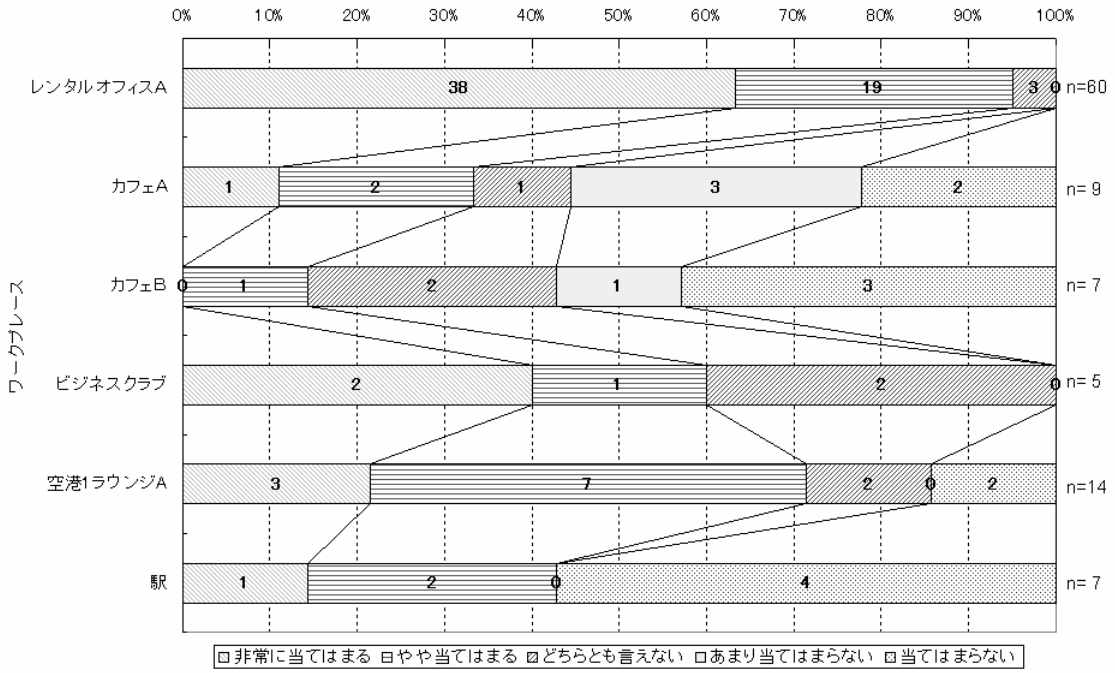

図 11 ワークプレースごとの安心度
Fig. 11 Reassurance of each workplace.

トメトリクス認証についてはまだ普及率は高くない．よって，盗難，紛失の恐れがなく，かつどの PC でも使えるような認証システムを取り入れる方向でも検討していく必要がある．

一方，システム側の情報セキュリティ対策が十分であっても必ずしもそれだけでは安心してシステムを利用できるとはいえない．その安心度は，ワークプレース，すなわちシステムの利用場所によって大きな差が生じることが分かった．今後は，情報を安心して扱うことができる作業環境のデザインについても検討していく方向である．

謝辞 本実験は経済産業省からの受託実験「平成 15 年度情報家電協調基盤整備事業」の一環として行った．実験に多大なご協力をいただいた，京浜急行電鉄株式会社，コクヨ株式会社，株式会社竹中工務店，日本航空株式会社，株式会社野村総合研究所，三菱地所株式会社，エヌ・ティ・ティ　アイティ株式会社，NTT コミュニケーションズ株式会社の皆様に感謝いたします．

参 考 文 献

1) 社団法人日本テレワーク協会：テレワーク白書 2003 (2004).
2) W.A. スピンクス：テレワーク世紀，日本労働研究機構 (1998).
3) 原田　保，松岡輝美：実践 SOHO・テレワーク，日科技連出版社 (1999).
4) 社団法人日本テレワーク協会：テレワーク人工等に関する調査研究報告書（要約版）（平成 13 年度版）(2003).
5) 平山信彦：ワークスタイルの変化と支援環境，信学技報，OFS98-46, pp.19–24 (1998).
6) 小豆川裕子，W.A. スピンクス：企業テレワーク入門，日経文庫 791，日本経済新聞社 (1999).
7) 本田新九郎，安野貴之，平沢純一，青木真理子，清水健太郎，津村　宏：テレワーク支援システムの設計と実装，電子情報通信学会講演論文集　基礎・境界，p.321 (2003).
8) 前田裕二，木村永寿，渡邊巧美：Digital Chatty Windows：つながり感通信を用いたテレワーク支援システムの提案，ヒューマンインタフェースシンポジウム 2002 論文集，pp.407–408 (2002).
9) 力武健次，菊池高広，永田　宏，浅見　徹：テレワーク勤務環境での情報セキュリティ (2002). http://www.kddilabs.jp/paper/ipsj63-telework-final.pdf
10) 上住　圭，中濱清志：ユビキタスオフィス実現のためのパソコン環境ローミング技術，ヒューマンインタフェースシンポジウム 2002 論文集，pp.745–748 (2002).
11) 飯塚重善，上住　圭，中濱清志，中嶌信弥：PC 環境ローミング技術（シェアード PC）の起動時間短縮と異機種対応，情報処理学会研究報告，UBI-3,

pp.745–748 (2004).
12) http://www.realvnc.com/
13) 岡田潤之，河東 勇，清水茂樹：サーバベースコンピューティング（SBC）ソリューション，三菱電機技報，Vol.77, No.4, pp.263–266 (2003).
14) http://www.citrix.co.jp/products/MFXP/metaframe.html
15) http://jp.sun.com/products/catalog/pdf/sunrayappliance.pdf
16) http://www.vmware.com/
17) 須崎有康：「ネットワークを渡り歩けるコンピュータ」の実装，情報処理学会研究報告，OS84-21, pp.149–156 (2000).
18) 須崎有康：「ネットワークを渡り歩けるコンピュータ」のチェックポイント機能，情報処理学会研究報告，OS88-4, pp.19–26 (2001).
19) Iizuka, S., Uwazumi, K., Nakahama, K., Nakajima, S. and Ogawa, K.: Secure PC Environment Roaming Technology for Ubiquitous Office, Ubicomp2003 (2003).
20) http://www.idk.co.jp/products/hdg/CDS/
21) 吉川肇子，白戸 智，藤井 聡，竹村和久：技術的安全と社会的安心，社会技術研究論文集，Vol.1, 1-8 (Oct. 2003).

(平成 16 年 6 月 17 日受付)
(平成 17 年 1 月 7 日採録)

飯塚 重善（正会員）

昭和 42 年生．平成 2 年静岡大学理学部数学科卒業．同年日本電信電話株式会社入社．現在，同社サイバーソリューション研究所研究主任．主に，ヒューマンインタフェースの研究に従事．電子情報通信学会，ヒューマンインタフェース学会各会員．

小川 克彦（正会員）

昭和 53 年慶應義塾大学大学院工学研究科修士課程修了．同年日本電信電話公社入社．現在，NTT サイバーソリューション研究所所長．主に画像情報システムの実用化，ヒューマンインタフェースの研究，ブロードバンドサービスや情報家電の研究開発に従事．工学博士．電子情報通信学会，人間工学会，HFES 各会員．

中嶌 信弥

昭和 32 年生．昭和 57 年慶應義塾大学大学院工学研究科修士課程修了．同年日本電信電話公社入社．横須賀電気通信研究所勤務．平成 2 年〜平成 3 年米国ロチェスター大学客員研究員．現在，NTT アイティ音声コミュニケーション事業部開発部長．主に，音声合成技術，ユビキタスサービスの研究開発に従事．工学博士．著書に『考える道具としての LISP 入門』（共著，共立出版），『未来ネット技術シリーズ 4 メディア処理技術』（共著，オーム社）日本音響学会，電子情報通信学会各会員．