2004－IS－89　(5)
2004／8／26

セキュアなテレワーク支援システムとシステム利用時の安心感についての考察

飯塚 重善 † 小川 克彦 † 中嶌 信弥 ††

† NTT サイバーソリューション研究所　†† エヌ・ティ・ティ　アイティ株式会社

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，情報機器のセキュリティに関する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など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セキュアなテレワーク支援システムを開発した．さらに，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ヶ月間行った．その結果，本システムの有効性およびセキュリティについて高い評価を受けた．また，システムの環境面での情報セキュリティの調査を行い，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．本論文では，本システムのシステム構成，処理内容，評価実験の結果および考察を述べる．

キーワード　テレワーク，PC環境ローミング，情報セキュリティ，安心

Secure Telework Support System and a Study about Reassurance at the time of System Use

Shigeyoshi IIZUKA † Katsuhiko OGAWA † Shinya NAKAJIMA ††

† NTT Cyber Solutions Laboratories

†† NTT-IT CO.,LTD.

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 secure 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.

Keyword　telework, PC environment roaming, information security, reassurance

1　はじめに

昨今，自宅など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，所謂「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行われてきている[1)]．このテレワークの形態を実施する場所で分類すると，自宅の書斎など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などを備えた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などを活用して，移動中にも効率よく仕事を行うモバイル型テレワークがある[1, 2)]．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，など具体的なメリットが認識されやすい．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的に変えなくても導入可能であることから，営業部門など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[2)]．

しかしながら，テレワークを推進する上では,「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挙げられている[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 など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．例えば，コンピュータはそれ自信に資産価値があるため，盗まれる可能性がある．また，ノート PC 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など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，ハードディスクなどの固定媒体も盗難に遭う可能性は CD-R などと同様と考えなければならない[3)]．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，さまざまな場所を仕事の場とする際，その場所によって，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，システム面のセキュリティ対策としては，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，上記のような情報機器に関する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 など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[4, 5)]による，セキュアな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．

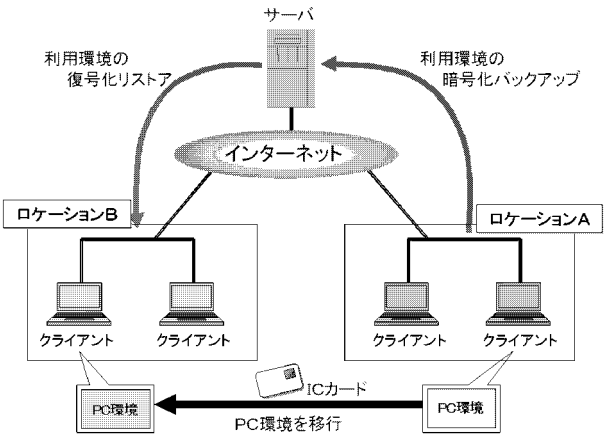

図 1: システムの全体構成

本論文では，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と，これを用いた評価実験の結果について述べる．

2 PC 環境ローミング技術

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 環境が，自動的にサーバにバックアップ・リストアされ，そのユーザが設定した PC 環境が共同利用パソコン上に再現される．

（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

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

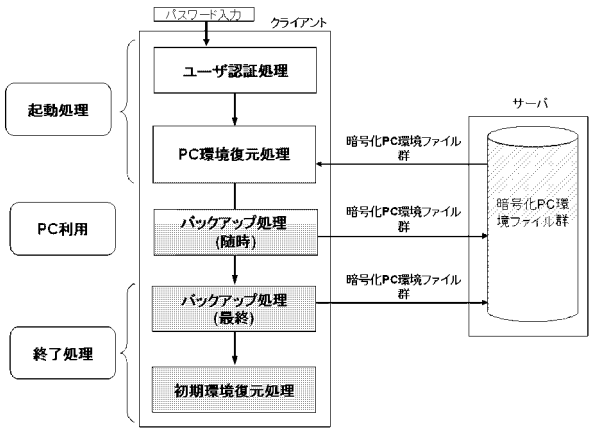

図 2: 概略フロー

ワーク（インターネット）上に配置される．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．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 項にその詳細を説明する．

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，“ システム用ユーザ ”と，“ 利用者用ユーザ ”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，“ システム用ユーザ ”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を行うと同時に Windows へのマージを行う．この後，“ 利用者用ユーザ ”にアカウントを切り替えて Windows を起動し直すことでそのユーザ環境での立

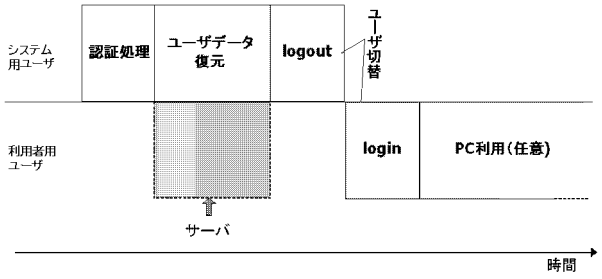

図 3: クライアント起動フロー

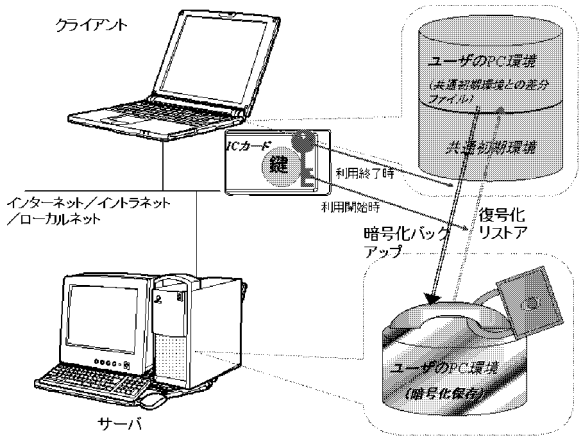

図 4: バックアップ処理

ち上げを実現している（図 3）．

3.2.3 バックアップ処理

自分が設定した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は容易に想像できる．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などを含む環境で，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．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など,「共通初期環境」との差分にあたる．本システムに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（Δ t）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，その都度，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+Δ t 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．

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 [6] 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の自動化を実現している．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．

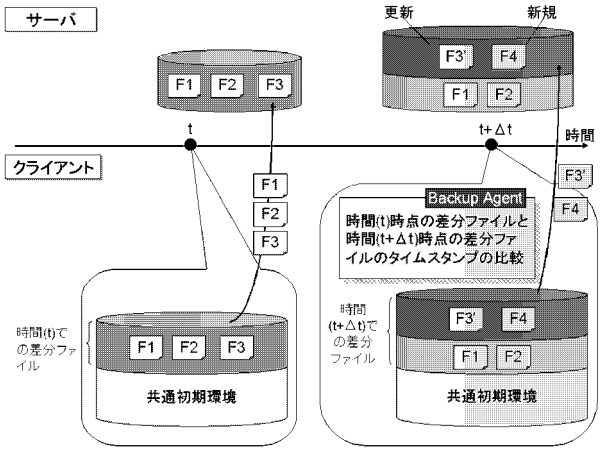

図 5: 定間隔差分バックアップ処理の詳細

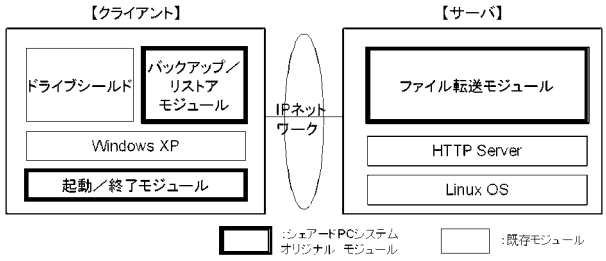

図 6: モジュール構成

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

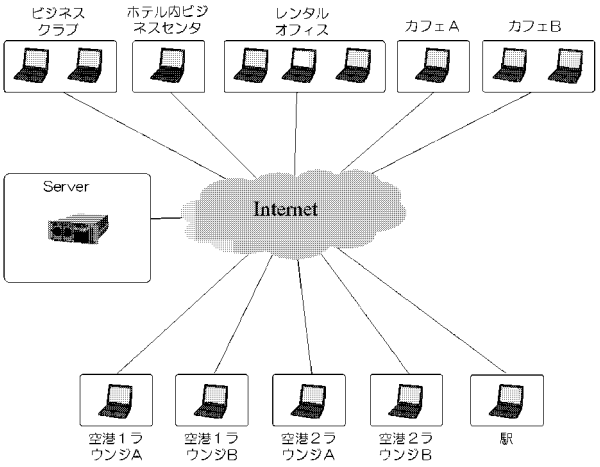

図 7: 実験構成

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．

4　実験

本システムを，実際のビジネスパーソンの業務に利用してもらうことで，テレワーク支援システムとしてのセキュリティ面の評価も含めた有効性の評価を実施した．併せて，ワークプレースによるシステム利用時の安心感の差についての調査を行った．

4.1　概要

本実験は，図 7 中に示したように，インターネット上にサーバを設置し，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ヶ月間実施した．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評価を行った．

4.2　結果及び考察

調査は実験終了後に質問紙を配布することで行った．全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．まず，システム利用に関するアンケートの質問および集計結果を図 8 に示す．

まず，質問 1 の結果から，本システムを今後も使

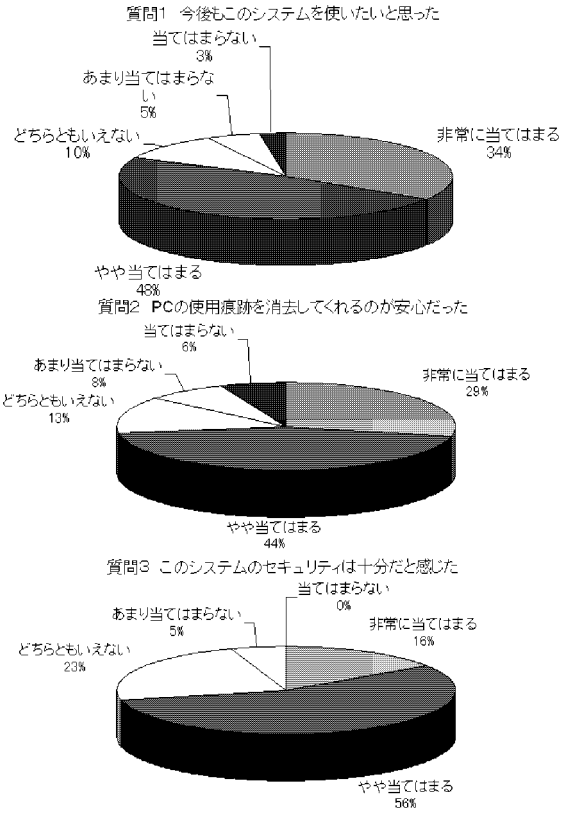

図 8: アンケート結果

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言える．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言える．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，セキュア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 で十分であると感じることができなかった 28% （22 人）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．全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．質問項目と集計結果を図 9 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わかった．そこで，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．

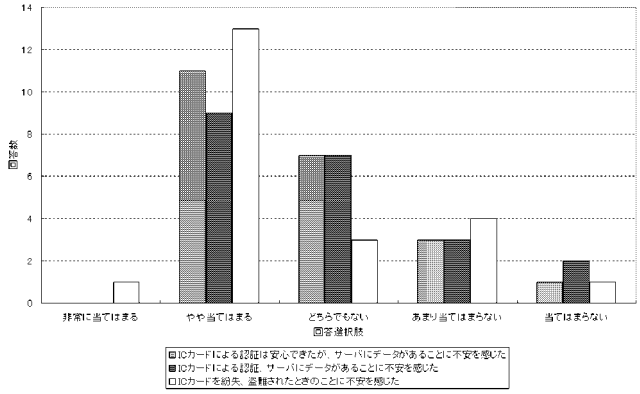

図 9: 本システムへの不安

また，サーバについては，今回の実験において，本システムのサーバが，いわゆるオープンなインターネット上に設置されたことに起因していると考えられる．実験に参加した企業において，その企業のセキュリティポリシー等の制約により，社内ネットワークへ接続することが許されなかったためである．これは単に,「実証実験」であるために社内ネットワークへの接続が会社によって認められなかったということではなく，個々の企業の持つセキュリティ維持の基準から見て，本実験で提供されるようなアウトソーシング型のシステム（社外に置かれた PC 環境ローミングサーバを介したサービス）がそもそも本質的に不可とされていることに依っていると考えられる．

4.3 利用時の安心度

一般的に，システムのセキュリティを高めることで安全性を確保するだけで，利用者が安心してそのシステムを利用できるとは言い切れない．因みに，社会技術的観点からも「安全」を「技術的に達成できる問題」とし，一方,「安心」とは,「安全とも大いに関わるけれどもそれだけでは決定できない，心理的な要素を含むもの」としている[7]．特に，本システムが対象としているテレワークについては，システムを利用する場所に不特定多数の人が行き来するようなパブリックスペースも含まれるため，システムを利用する場所に対する心理的な要素が利用時の安心感に影響を与える重要な要素であると考えられる．そこで我々は，心理的な要素として特に，扱っている情報を周りの人から見られることへの不安が大きいと考え，今回の実験の拠点となったワークプレースについて，モニタの，その場所の安心感として，周りの人から見られることへの不安を重点的に調査することとした．調査の方法は，今回の実験モニタ 77 名に，以下に示すような，利用時の安心感や何が気

表 1: 各ワークプレースの形態

ワークプレース	右側	左側	後側	人通り
レンタルオフィス	P	P	P	少
カフェ A	隣席	隣席	通路	少
カフェ B	隣席	壁	通路	多
ビジネスクラブ	隣席	壁	通路	少
空港ラウンジ	隣席	隣席	通路	少
駅	通路	隣席	壁	多

P：パーティション

になったかについて，各ワークプレース答えてもらうことで評価した．なお，調査の対象としたワークプレースは，5 人以上のモニタが利用したワークプレース（6 カ所）とした．そのワークスペースの一覧と，それぞれのワークプレースの形態およびワークプレースの周りの人通りの量を表 1 に示す．

質問 4　安心して作業することができた
質問 5　PC 画面を他の人に見られないか気になった
質問 6　パーティションの高さは適切だった
質問 7　後や横を通る人が気になった
質問 8　人通りの多さが気になった
質問 9　隣の席との距離は適切だった

まず，各ワークプレースでの安心感（質問 4）についての集計結果を図 10 に示す．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．この結果から，レンタルオフィス，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決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 節で示したように高いにも関わらず，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．すなわちこれは，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言える．

この結果から，レンタルオフィスのように，パーティションに囲まれ，もともとワークスペースとして設置されている場所についてはもちろん安心して作業できると感じることができ，ビジネスクラブも

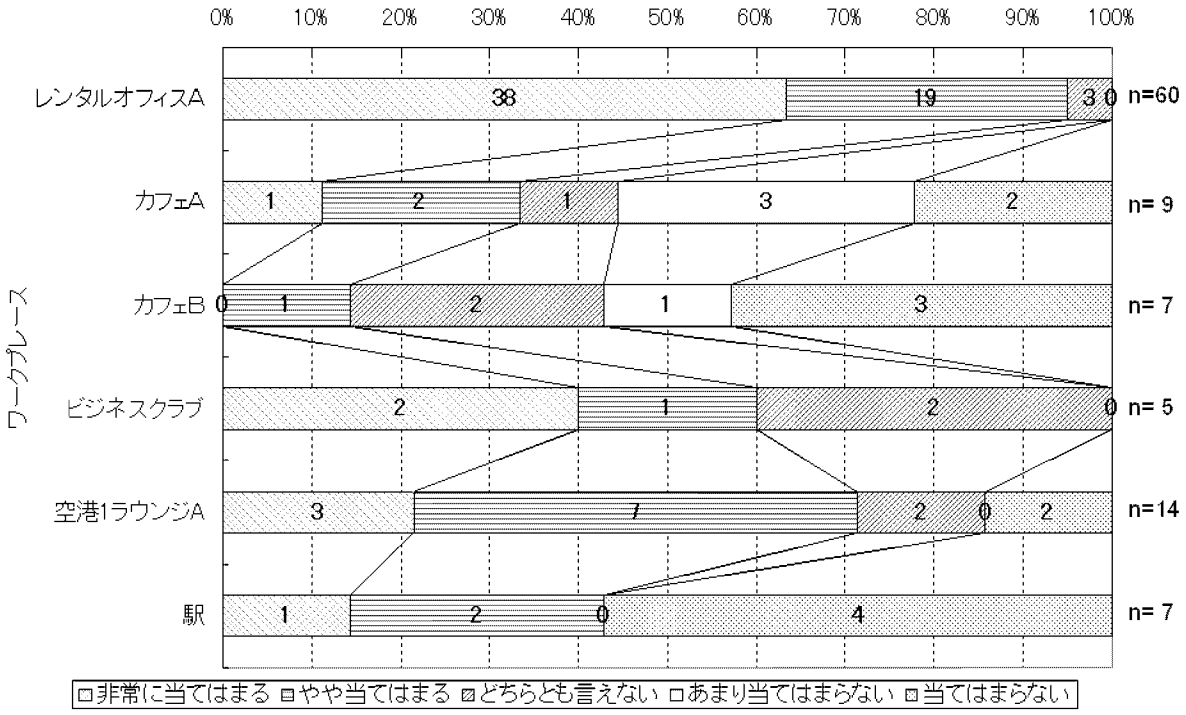

図 10: ワークプレース毎の安心度

ビジネスマンを対象としているため，比較的安心な環境と言えるようである．しかし，それ以外の場所については隣や通路との関係により，必ずしも安心な環境とは言えないようである．4.2 節で述べたようにシステム自体のセキュリティは十分であると感じていても，利用時に安心と感じるかどうかは，少なくともテレワークにおいては，その作業を行う場所の形態に依存するということが明らかになった．

また，PC 画面が見られることへの不安（質問 5）についての集計結果を図 11 に示す．これから，やはり前述の各ワークプレースでの安心感に関する結果で，必ずしも安心とはいえない環境という結果がでた場所については，PC 画面を見られることへの不安が大きいことが分かる．

次に，ワークスペースの形態や人通りについて（質問 6〜9），モニタの感じ方を見てみることとした．パーティションの高さや隣の席との距離の適切さや後や横を通る人，人通りの多さが気になったかの質問それぞれの回答の平均値を算出し，これを安心度としてレーダーチャートにしたものを図 12 に示す．

この結果から,「安心して作業ができた」について評価が高かったワークプレース（レンタルオフィス・ビジネスクラブ）の特徴を見てみると,「パーティションの高さが適切だった」と「隣の席との距離が適切だった」の 2 項目の評価も高くなっている．すなわち,「安心して作業ができる環境」については,「パーティションの高さの適切さ」や「隣の席との距離」といった「環境の設備面」の条件が影響すると考えられる．

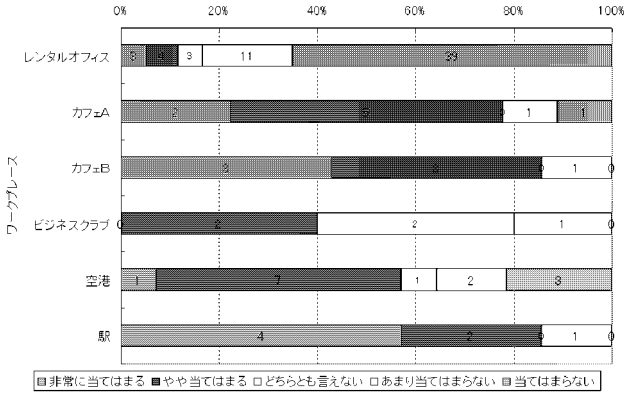

図 11: PC 画面を見られることへの不安

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セキュアな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うことでセキュリティ面も含めたテレワーク支援システムとしての

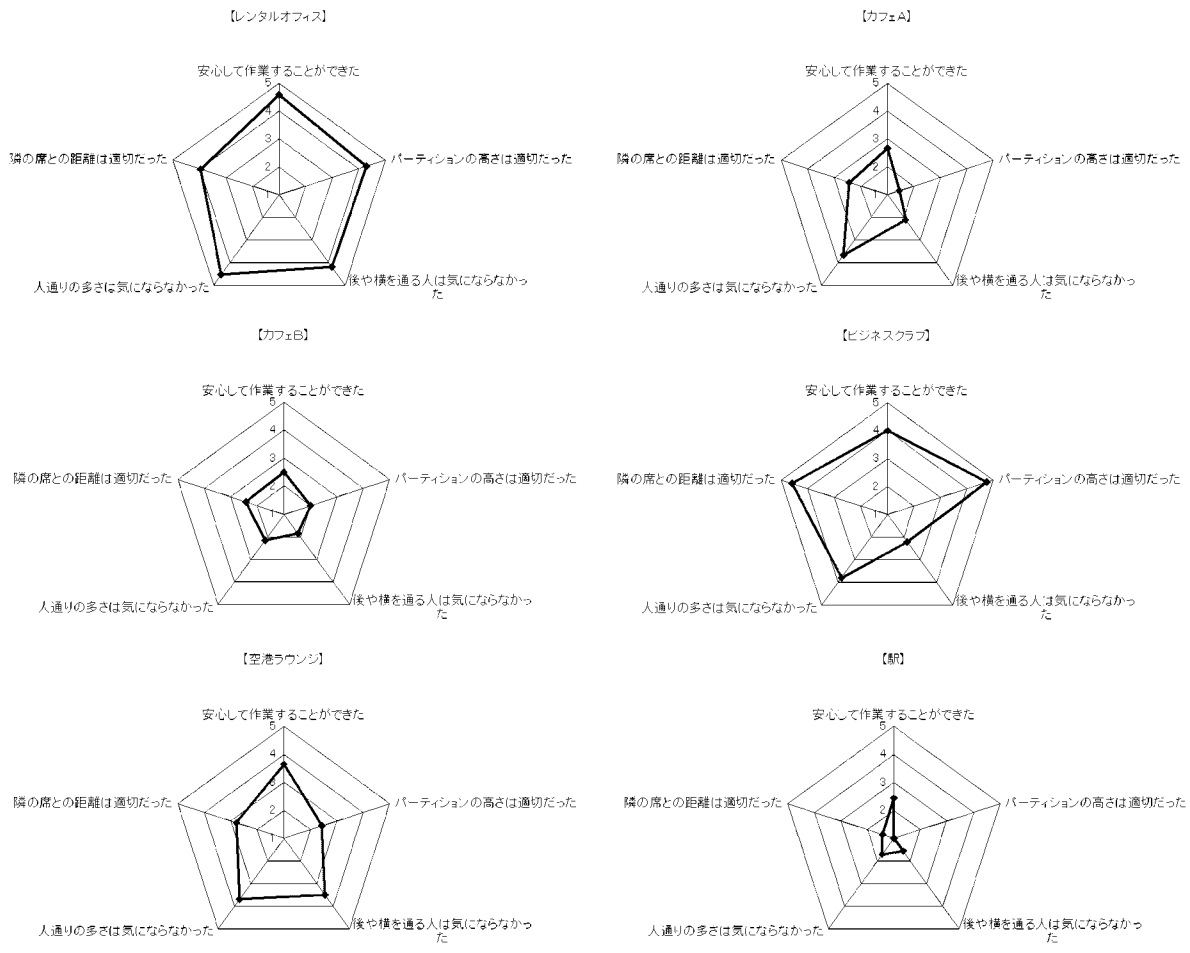

図 12: ワークプレース毎の安心度要因

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．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言えない．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，我々は，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．

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) 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).

3) 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, http://www.kddilabs.jp/paper/ipsj63-telework-final.pdf (2002).

4) 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).

5) 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, 情処研報, UBI–3, pp.745–748 (2004).

6) “ http://www.idk.co.jp/products/hdg/CDS/ ”

7) 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)